وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني وسبل مواجهتها من منظور طريقة خدمة الجماعة

Awareness of University Students About the phenomenon of Electronic Blackmail and Ways to Face It from The Perspective of Social Group Work

الدكتور علي بن سهيل تبوك

أستاذ مساعد علم الاجتماع الرقمي

قسم العلوم الاجتماعية –كلية الآداب والعلوم التطبيقية –جامعة ظفار

الدكتور محمد محمد بسيوني قنديل

استاذ العمل مع الجماعات بكلية الخدمة الاجتماعية جامعة حلوان

استاذ العمل الاجتماعي المساعد بكلية الآداب والعلوم التطبيقية جامعة ظفار

ملخص الدراسة

تهدف الدراسة الحالية إلى تحديد مستوى وعي طلبة الجامعة بظاهرة الابتزاز الإلكتروني من خلال تحديد مستوى معرفة طلبة الجامعة بظاهرة الابتزاز الإلكتروني، وتحديد مستوى اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الإلكتروني، وتحديد مستوى الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الإلكتروني، بالإضافة إلى محاولة التوصل إلى سبل مقترحة من منظور طريقة خدمة الجماعة لمواجهة ظاهرة الابتزاز الإلكتروني لدى طلبة الجامعة ، واعتمدت الدراسة على عينة عشوائية مُمثلة لمجتمع الدراسة ضمّت 60 طالبًا وطالبة من أعضاء مجموعة العمل الاجتماعي بقسم العلوم الاجتماعية، كلية الآداب والعلوم التطبيقية، جامعة ظفار بسلطنة عمان، في العام الدراسي 2024/2023م ، وتوصلت الدراسة إلى عدد من السبل المقترحة، منها تشكيل فريق من جماعات الطلبة المتطوعين المهتمين بنشر الوعي حول ظاهرة الابتزاز الإلكتروني، وتدريب أعضاء الفريق بشكل مكثف لتنظيم الحملات التوعوية داخل الجامعة باستخدام مختلف الوسائل، تنظيم حملات توعية على منصات التواصل الاجتماعي للطلاب والمجتمع الجامعي حول ظاهرة الابتزاز الالكتروني وكيفية الوقاية منها.

الكلمات الدالة : الابتزاز ــ الابتزاز الالكتروني

Study Summary:

The current study aims to determine the level of awareness among university students regarding the phenomenon of electronic Blackmail by identifying their knowledge level of such phenomenon, assessing their attitudes towards the phenomenon of electronic Blackmail, and identifying their actual practices in dealing with these phenomena. Additionally, the study attempts to propose Ways, From the Perspective of Social Group Work, to confront the phenomenon of electronic Blackmail among university students. The study adopted a random representative sample of the study population, which included 60 male and female students who are members of the Social Work Group at the Department of Social Sciences, College of Arts and Applied Sciences, Dhofar University in the Sultanate of Oman, in the academic year 2023/2024. The study has concluded several proposed approaches, including forming a team of volunteer student groups interested in raising awareness about the phenomenon of cyberbullying, intensive training of team members to organize awareness campaigns within the university using various means, organizing awareness campaigns on social media platforms for students and the university community about cyberbullying and how to prevent it

Keywords: Blackmail – Electronic Blackmail

أولا : مشكلة الدراسة:

شهد العالم تقدمًا كبيرًا في شتى الميادين، بما في ذلك مجال تكنولوجيا المعلومات، وشبكة الإنترنت وتطبيقاتها المتقدمة، ولقد سهَّلت هذه التطورات التواصل والتقارب بين الأفراد في أي مكان في العالم، مما جعل العالم يبدو وكأنه قرية صغيرة بفضل توسع صناعة الإنترنت وزيادة أعداد مستخدميها في جميع أنحاء العالم. (الرويس، 2020، ص 80)

كما يظهر بوضوح أن التقنية ووسائل الاتصال تلعب دورًا مهمًا في حياة الناس ، حيث تمتلك إمكانيات فعَّالة في نقل الثقافة وتشكيلها بين أفراد المجتمع. كما ساهمت في تغيير الكثير من الاتجاهات والسلوكيات وتصرفات الأفراد، ولذلك تُعتبر سلاحًا ذو حدين. فعلى الرغم من أنها سهلت وطورت حياة الإنسان بشكل واضح، إلا أنها لا تخلو من وجود ثغرات وجوانب سلبية أثرت على الفرد والمجتمع. حيث أدى التطور التكنولوجي إلى ظهور المشكلات التي يعاني منها المجتمع اليوم .(الحربي وسليمان، 2022، ص 2)

من بين المشكلات الرئيسية التي تعاني منها العالم اليوم نتيجة التقدم التقني، تظهر مشكلة الابتزاز الإلكتروني بوضوح. فقد أصبحت قضية الابتزاز الإلكتروني ظاهرة عالمية، تمتلك أبعادًا انسانية واجتماعية متعددة، وقد فرضت نفسها في وقتنا الحاضر على جميع المجتمعات بغض النظر عن درجة تقدمها. إنها قضية تزداد أهميتها مع مرور الزمن. (أبو زيد، 2002، ص 3) ، كما يعتبر الابتزاز الإلكتروني من بين الجرائم الصعبة التي تكتنفها الغموض أثناء مراحل ارتكابها، خاصةً أنها تُنفذ عادةً من قِبل أشخاص يمتلكون دراية كافية في استخدام تقنيات المعلومات. بالإضافة إلى ذلك، يتميز مرتكبو هذه الجرائم بصفات تختلف عن تلك لمرتكبي الجرائم التقليدية. كما أن التطور الحاصل في مجال تكنولوجيا المعلومات يتطلب استخدام أساليب تحقيق متطورة وجمع أدلة متقدمة. وبالتالي، يحتاج فريق التحقيق المكلف بمثل هذه القضايا إلى وجود خبراء ومتخصصين ضمن تشكيلته. (موسى، 2022، ص 237)

أشارت دراسة (شعيبت والسعدى، 2023، ص50) إلى أن الابتزاز الإلكتروني يُعتبر جريمة دولية لأنها عابرة للحدود، وأن المجني عليه في هذه الجرائم غالبًا ما يكون هو السبب في تعرضه للابتزاز، سواءً بسبب قلة وعيه أو عدم معرفته الجيدة باستخدام التقنيات الحديثة، أو بسبب الثقة الزائدة بالجاني المبتز. كما أن جريمة الابتزاز الإلكتروني تُعتبر من بين أكثر أنواع الجرائم المعلوماتية انتشارًا في الوقت الحالي، حيث تُمثل عملية ترهيب وتهديدًا لفئات المجتمع.

وأكدت دراسة (الحربي وسليمان، 2022، ص 25) على أن قضية الابتزاز تتلخص حول التهديد بكشف معلومات عن شخص أو فعل شيء مدمر له لتدميره إذا لم يستجب لبعض الطلبات. تكون هذه المعلومات عادةً محرجة أو ذات طبيعة مدمرة اجتماعيًا. يحاول الشخص المبتز الحصول على مكاسب مادية أو معنوية عن طريق الإكراه من شخص آخر، ويتم ذلك عن طريق التهديد بفضح سر من أسرار الشخص المعني بالابتزاز أو نشر صور أو مقاطع فيديو. ونظرًا لأن جريمة الابتزاز ترتبط مباشرة بالأعراض، فإنها تثير قلقًا في المجتمع وتهديدًا للأمن الأخلاقي فيه.

كما توصلت دراسة (شعيبت والسعدى، 2023، ص 53) إلى أن جريمة الابتزاز الالكتروني تتمتع بطرق مختلفة في ارتكابها، ولها وسائل خاصة بها تختلف عن الابتزاز التقليدي. يمكن أن تستهدف هذه الجريمة النساء والرجال والأطفال، بالإضافة إلى الشخصيات المعنوية لتحقيق الكسب المادي، وهي جريمة عابرة للحدود، حيث يمكن أن يكون المبتز في دولة بعيدة، ويقوم بابتزاز ضحيته في أقصى العالم.

ويُلاحظ أن الابتزاز الإلكتروني قد فرض نفسه كقضية حديثة تواجه المجتمعات على اختلاف أعراقها. والتي حاولت بذل العديد من الجهود القانونية التخفيف من تفاقم هذه المشكلة، من خلال سن وتطوير القوانين والتشريعات الرادعة. يأتي ذلك نظرًا للانعكاسات الخطيرة التي تترتب على هذه القضية، ليس فقط على المستوى الفردي، بل أيضًا على مستوى الأسرة والمجتمع.(النوفلي واللويهية ، 2019 ، ص 20)

وأكدت دراسة (Mohamed, 2022) على ذلك، حيث أشارت إلى التطور الكبير في تكنولوجيا المعلومات والتحول الرقمي، وأظهرت أن التحول الرقمي قد زاد من انتهاك الخصوصية عبر الإنترنت. وبناءً على ذلك، أكدت على الضرورة والحاجة إلى إصدار تشريعات لمواجهة كافة أنواع الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني.

وانطلاقًا من حقيقة أن الابتزاز الإلكتروني يُعد من أخطر الجرائم التي تسبب للضحية أضرارًا جسيمة، سواء على المستوى المهني أو الاجتماعي أو الخاص، فقد حرصت الكثير من الدول والحكومات على مواجهته، واتخذت كافة الإجراءات اللازمة لمنع وقوعه وفرض العقوبات على الجاني. ومن بين هذه التشريعات قانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية

المتحدة، وقانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات في مصر، وقانون مكافحة جرائم المعلوماتية الأردني لعام 2015 وتعديلاته لعام 2018.(Mohamed and Others, 2022) ، كما عالج المشرع العراقي ظاهرة الابتزاز الإلكتروني من خلال عدد من النصوص في قانون العقوبات، حيث قد يترتب على مخالفتها حكم بالسجن أوالغرامة المالية،وفقًا لنوع الجريمة.(حنون، 2023، ص 80)

هذا ويجرم المشرّع العُماني الابتزاز الإلكتروني في المادة (18) من قانون مكافحة جرائم تقنية المعلومات بعقوبات حبسية تمتد من شهر وحتى ثلاث سنوات، وغرامة تصل إلى ثلاثة آلاف ريال. ويشدد المشرّع هذه العقوبة إلى السجن من ثلاث سنوات حتى عشر، والغرامة حتى عشرة آلاف ريال، إذا كان التهديد يتضمن ارتكاب جناية أو تشهيرًا بأمور مخلة بالشرف والاعتبار. كما يتولى الادعاء العام التحقيق في جرائم الابتزاز الإلكتروني، ويستعين في ذلك بشركاء رئيسين وهم: شرطة عُمان السلطانية، ومختبرات الأدلة الرقمية، بالإضافة إلى مزودي خدمات الإنترنت. ومع ذلك، يجب الاعتراف بأن الابتزاز الإلكتروني يُعد من بين أصعب التحقيقات، لا سيما إذا كان الجاني خارج السلطنة، حيث قد لا يكون الوصول إليه ممكنًا بشكل فوري، مما يعرض الضحية للخسائر المالية أو التشهير عبر الإنترنت قبل أن يتم التحقيق.(المقبالى، 2019، ص 91)

وفي خضم ثورة المعلومات والتكنولوجيا، ومع سهولة الوصول إلى الإنترنت وانتشار مواقع التواصل الاجتماعي، أصبح طلاب الجامعة عرضة للابتزاز الإلكتروني، لأسباب متعددة، منها قلة وعيهم بظاهرة الابتزاز الإلكتروني، وثقتهم الزائدة في الآخرين، وسهولة مشاركة المعلومات الشخصية على الإنترنت، وعدم اتخاذهم الإجراءات اللازمة لحماية أنفسهم من الابتزاز.

وتؤكد الدراسات الحديثة على خطورة هذه المشكلة على الطلاب، ومنها دراسة (Taşkın and Others, 2022) التي أكدت على تعدد العوامل التي تزيد من خطر تعرض الطلاب للجرائم الإلكترونية، ومنها استخدامهم لوسائل التواصل الاجتماعي بشكل أكبر من غيرهم، بالإضافة إلى عدد الصداقات التي يقومون بإقامتها عبر الإنترنت.

كما هدفت دراسة (Roderic وآخرون، 2022) إلى تقييم مخاطر الجرائم الإلكترونية لطلاب الجامعات من خلال تعريضهم لأنواع مختلفة من رسائل البريد

الإلكتروني الاحتيالية ومراقبة ردودهم، ومعرفة مدى وعيهم بهذه المخاطر من أجل تطوير استراتيجيات الحماية. وأكدت دراسة (Chantal وآخرون، 2022) أن الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني، أصبحت قضيةً ناشئة في سياق التعليم العالي، خاصةً مع تزايد ادماج تقنيات المعلومات والاتصال (ICT) في الحياة اليومية بالجامعة.

وبناءً على ما سبق، يُمكن القول إن جريمة الابتزاز الإلكتروني تمثل مشكلة خطيرة يجب على مختلف المهن الإنسانية والاجتماعية وكافة المؤسسات الاجتماعية التصدي لها بقوة. تُشكل مهنة الخدمة الاجتماعية خط الدفاع الأول في حماية المجتمع من مخاطر هذه المشكلة، حيث يمكن للأخصائي الاجتماعي أن يلعب دورًا محوريًا في التصدي لها ونشر الوعي بمخاطرها، من خلال تنظيم الندوات وورش العمل المختلفة في الجامعات والمدارس والمجتمعات المحلية، ونشر المواد التوعوية حول ذلك. وهذا ما أشارت إليه دراسة (أبو زيد، 2002، ص 3) والتي استهدفت التعرف على واقع ممارسة الأخصائي الاجتماعي لاستخدام نموذج الأزمة مع ضحايا الابتزاز الإلكتروني من طلبة المرحلة الثانوية. ومن أهم نتائجها تقديم برنامج مقترح يمثل دليلًا إرشاديًا للأخصائيين الاجتماعيين العاملين في المدارس الثانوية عند التعامل مع مشكلة الابتزاز الإلكتروني للطلبة، من خلال الاستفادة من نموذج التدخل في الأزمات.

كما أكدت دراسة (الحربي وسليمان، 2022، ص 27) على دور كبير لمهنة الخدمة الاجتماعية في رفع مستوى الوعي المجتمعي بجرائم الابتزاز الإلكتروني لدى طالبات جامعة الملك عبد العزيز من خلال تعزيز القيم المجتمعية والانتماء وحب العمل والتعاون، وتعزيز الأمن المجتمعي وحمايته من جميع الجرائم الإلكترونية، وخاصة جرائم الابتزاز الإلكتروني. كما أوصت الدراسة بإجراء المزيد من الدراسات والبحوث في مجال تعزيز دور الخدمة الاجتماعية في الحد من جرائم الابتزاز الإلكتروني لدى الطالبات في جامعات أخرى، وتوجيه التدريب للأخصائيين الاجتماعيين للتعامل مع ضحايا الابتزاز الإلكتروني وتزويدهم بالبرامج الوقائية والمساعدة في تجاوز المشكلة، وزيادة الحملات التوعوية للطالبات في الجامعة حول جرائم الابتزاز الإلكتروني وكيفية التصرف في حال التعرض لها، وإعداد دليل إرشادي من قبل الجامعة لمكافحة جرائم الابتزاز الإلكتروني يوزع على طالبات الجامعة بهدف توعيتهن وحمايتهن من الوقوع في المشكلة.

هذا وتستطيع طريقة خدمة الجماعة، كإحدى طرق مهنة الخدمة الاجتماعية، أن تلعب دورًا فعالًا في توعية طلبة الجامعة بظاهرة الابتزاز الالكتروني من خلال البرامج الجماعية التي تهدف إلى تنمية القيم الإيجابية بينهم وزيادة خبراتهم ومعلوماتهم.

وهذا ما اكدته نتائج دراسة (ابراهيم،2022، ص 170) حيث اشارت الي احتياج الشباب الجامعى لأنشطة البرامج الجماعية من أجل إشباع إحتياجاتهم وتزويدهم فكرياً بالمعلومات والمعارف والمهارات التكنولوجية التي تُساعدهم على تنمية الوعى لديهم، كما اكدت علي اهمية التقويم المستمر للبرامج الجماعية للشباب الجامعي للوقوف على مدى تحقيق الأهداف منها، مراعاة تدرج البرامج الجماعية من الأسهل الى الأكثر تعقيداً مما يساعد على نمو الخبرات لدى الشباب الجامعي .

وتمثل الجامعات كأحد أهم المؤسسات التعليمية في المجتمع وسيلةً هامةً لتحقيق أهداف طريقة خدمة الجماعة من خلال مواجهة ظاهرة الابتزاز الإلكتروني. يتم ذلك عن طريق نشر الوعي حول هذه الظاهرة بين جماعات الطلبة، من خلال تنظيم ندوات وورش عمل، وتقديم برامج توعوية تهدف إلى تنمية مهارات الطلبة في التعامل مع الإنترنت بأمان. كما يتم توفير الدعم النفسي والاجتماعي للطلبة ضحايا الابتزاز الإلكتروني، بالإضافة إلى التعاون مع الجهات المختصة لمكافحة جرائم الابتزاز الإلكتروني". وأكدت علي ذلك دراسة (الحجري، 2019، ص 11)، حيث أشارت إلى أن للجامعات دورًا هامًا في تعريف جماعات الطلبة بظاهرة الابتزاز الإلكتروني ، والمساهمة في تطوير سياسات وبرامج محو الأمية الرقمية في مجال تقنيات المعلومات والاتصالات.

كما قدمت العديد من الدراسات والبحوث السابقة عددا من المقترحات والتوصيات التي تبين اهمية الوعي لدي فئات المجتمع وخاصة طلبة الجامعة في سبيل التصدي لتلك الظاهرة ومنها دراسة (الخالدى، 2020، ص 2066) والتي توصلت الي عدد من النقاط المهمة والتي لها دور بارز في عملية تعزيز الوعي الاجتماعي لدى فئات المجتمع والتي تتمثل في : تجنب طلب الصداقات أو قبول طلب الصداقة من قبل أشخاص غير معروفين، عدم الرد والتجاوب على أي محادثة ترد من مصدر غير معروف ، ابلاغ الجهات الرسمية في حالة التعرض للابتزاز الالكتروني ، عدم الاحتفاظ بأي حسابات بنكية او صور شخصية أو صور عائلية أو معلومات ذات خصوصية على أي حساب سواء على الكمبيوتر الشخصي أو اللوحي او الهاتف المحمول، حيث إن أي اختراق لأي حساب سيستتبع اختراق بقية الأجهزة وهو ما يجعل الاحتفاظ بالبيانات الشخصية على تلك الأجهزة خطيرا للغاية.

كما أوصت دراسة (موسى، 2022، ص 237) بضرورة إنشاء أجهزة أمنية وقضائية متخصصة لمكافحة جرائم الابتزاز، بالإضافة إلى خضوع رجال التحقيق لبرامج تدريبية بشكل دوري تساعدهم على تحديث معرفتهم والاطلاع على آخر التطورات في مجال تكنولوجيا المعلومات. كما تحث الدراسة على العمل الجاد في مجال التحقيق بين الدول من خلال إبرام الاتفاقيات والمعاهدات الثنائية والمتعددة الأطراف.

وفي محاولة أخرى لمنع الابتزاز عبر الاتصالات المتنقلة، اقترحت دراسة (Chin-Ling, Chen., Ming-He, Liu., 2011) حلاً يعتمد على وجود توقيع رقمي يمكن من خلاله تتبع الحساب الذي حدده المجرم أثناء عملية الابتزاز. كذلك، أكدت دراسة (Chin and Others, 2022) على أهمية الاعتماد على نظام تحويل النقد الإلكتروني القابل للتتبع ضد الابتزاز على الهواتف المحمولة.

كذلك أشارت دراسة (الحسيني، 2023، ص 383) إلى وجود علاقة إيجابية بين التفكك الأسري وضعف الوازع الديني من جهة، والإقبال على الابتزاز الإلكتروني. وقد سلطت الدراسة الضوء على مجموعة من التوصيات التي تدفع الحكومات لأداء دورها من خلال البرامج والنظم الإلكترونية الكاشفة للجناة، وتشديد العقوبات. ومن بين هذه التوصيات، حث الجامعات والمراكز البحثية على البحث والدراسة في الجرائم المعلوماتية والجرائم عبر الإنترنت، ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم. كما دعت إلى تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية، وإنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.

كما أوصت دراسة (حنون، 2023، ص 87) بزيادة آليات التعاون الدولي لمواجهة جريمة الابتزاز الإلكتروني، من خلال تشديد التشريعات الجنائية وعقوباتها، واتخاذ التدابير اللازمة لتعقب الجناة واعتقالهم. كما دعت إلى ضرورة توعية الجمهور بمخاطر جريمة الابتزاز والتحذير من السلوكيات التي قد تجعل الشباب عرضة للابتزاز، من خلال حملات توعوية في وسائل الإعلام المختلفة ، وأيضًا أوصت دراسة (النوفلي واللويهية، 2019، ص 38) بتحديد جهة مختصة بالنظر في الإبلاغ عن حالات الابتزاز، بدلاً من التعامل مع الموضوع من قبل عدة جهات مختلفة. كما اقترحت تحضير مادة فيلمية تتضمن عرضًا مرئيًا عن الجريمة، وتكليف الأخصائي الاجتماعي بعرضها على

الطلاب خلال حصص إرشادية في المدارس. ودعت إلى توعية مجالس الآباء والأمهات للمساهمة في توعية الأبناء، وإعداد كتيب توعوي يشرح كيفية التصرف عند تعرضهم للابتزاز، وتوزيعه على جماعات الطلاب في المدارس، خاصة الصفوف من الصف العاشر فصاعدًا.

كما قدمت دراسة (الشكيلية، 2019، ص 60) مجموعة من المقترحات للوقاية من جريمة الابتزاز الإلكتروني، حيث تمثل الوقاية الحل الأمثل للحد منها. ومن بين هذه المقترحات: رفع وعي الوالدين وتشجيعهم على بناء علاقات متينة وثقة مع أطفالهم، وتعزيز الثقة بينهم لتشكيل رابط نفسي قوي يحمي الطفل من الوقوع في فخ الابتزاز الإلكتروني، وزيادة وعي الأطفال بالجريمة وتعريفهم بالإجراءات الواجب اتباعها إذا تعرضوا لها ، ويمكن أيضًا تقديم الندوات والمحاضرات لطلاب المدارس لتعريفهم بمخاطر الابتزاز الإلكتروني والعواقب القانونية له، وذلك لبناء حاجز نفسي يحد من احتمالية تورط الطلاب في هذه الجريمة.

كما هدفت دراسة (الغديان وآخرون، 2018، ص 50) إلى الكشف عن أهم صور جرائم الابتزاز الإلكتروني ودوافعها، والآثار النفسية المترتبة عليها، وكانت من توصياتها التركيز على التنشئة الاجتماعية السليمة وتعزيز القيم الدينية والأخلاقية لدى جماعات الشباب، من خلال تنمية الرقابة الذاتية وتفعيل دور الأسر في رقابة سلوك الأبناء ومراحل نموهم. كما دعت الدراسة إلى الاهتمام بمراكز الشباب التي تعنى بالجانب الوقائي والترفيهي، وتلبية طموحاتهم، وتحقيق دوافعهم، وتشبع حاجاتهم العاطفية، مثل بناء العلاقات الاجتماعية وإنشاء شبكات التواصل الاجتماعي.

كما استهدفت دراسة (الرويس، 2020، ص 86) الوقوف على درجة الوعي بالآثار الاجتماعية لظاهرة الابتزاز الإلكتروني لدى الأسر في المجتمع السعودي، وقدمت الدراسة عددا من التوصيات من أهمها التركيز على البرامج التوعوية التي تهدف إلى بيان مخاطر الابتزاز الإلكتروني على الفرد والأسرة والمجتمع، بالإضافة إلى تفعيل الجوانب الوقائية من خلال إنشاء حسابات في شبكات التواصل الاجتماعي تعنى بنشر الوعي المجتمعي والتثقيف بمخاطر جريمة "الابتزاز الإلكتروني". وأشارت الدراسة إلى ضرورة عقد اللقاءات والندوات والمؤتمرات العلمية لمناقشة مشكلة الابتزاز الإلكتروني، وتفعيل الأنظمة والقوانين التي تسعى إلى الحد من انتشار الابتزاز الإلكتروني واستغلال الضحايا ماديًا أو معنويًا من قبل الأشخاص المبتزين.

وأوصت دراسة (حسين، 2019) بالعمل على زيادة الوعي القانوني لدى فئات المجتمع، خاصة الشباب المستخدمين للشبكة المعلوماتية أو وسائل تقنية المعلومات مثل الهواتف المحمولة وغيرها، بمخاطر إساءة استخدام تلك الوسائل على سلامة المجتمع وأفراده، والعقوبات التي تطالهم في حال قيامهم بذلك، أو مساعدة من يقوم بتلك الأفعال، وخطورة الانزلاق في العلاقات عبر وسائل التواصل الاجتماعي المختلفة، وكذلك الكشف عن الأسرار أو المعلومات أو البيانات أو الصور الخاصة بهم.

كما توصلت دراسة (إبراهيم، 2022، ص 195) إلى مجموعة من التوصيات، منها العمل على تقديم دورات تدريبية للشباب الجامعي من خلال إدارة رعاية الشباب في الكليات، والسعي إلى تقوية الوازع الديني لدى جماعات الشباب الجامعي من خلال عقد الندوات بشكل دوري، واستخدام وسائل الإعلام المختلفة لتوعية الشباب الجامعي بالآثار السلبية الناجمة عن كثرة استخدام مواقع التواصل الاجتماعي.

وبناءً على ما سبق، يؤكد الباحثان على أهمية طريقة خدمة الجماعة في زيادة وعي طلبة الجامعة بالجرائم الإلكترونية، خاصة الابتزاز الإلكتروني، وذلك في ظل التحول السريع والمتزايد لاستخدام مواقع التواصل الاجتماعي بين جماعات الشباب الجامعي. ونظرًا للمخاطر المتزايدة للابتزاز الإلكتروني على مستخدمي مواقع التواصل الاجتماعي بشكل عام، وعلى طلاب الجامعة بشكل خاص، وما يصاحب ذلك من مشكلات وسلبيات على المجتمع وأفراده، جاءت الحاجة إلى أهمية الوقوف على مستوى وعي طلبة الجامعة بظاهرة الابتزاز الإلكتروني.

ومن ثم، يمكن للباحثان صياغة مشكلة الدراسة على النحو التالي: ما مستوى وعي طلبة الجامعة بظاهرة الابتزاز الإلكتروني ؟"

ثانيا : اهمية الدراسة

1. تستمد الدراسة أهميتها من موضوع الابتزاز الالكتروني لدى طلبة الجامعة، والذي يُعدّ ظاهرة خطيرة تُهدّد أمن واستقرار المجتمع.
2. كما تكتسب الدراسة أهميتها من تركيزها على فئة الشباب الجامعي، الذين يتمتعون بالحماس والحيوية واستخدامهم لوسائل التواصل الاجتماعي بصورة متزايدة، ممّا يُعرّضهم لمخاطر الابتزاز الالكتروني الناتج عن سوء استخدام هذه الوسائل.

3. وتأتي هذه الدراسة استجابة لتوصيات بعض الدراسات السابقة التي أكدت على ضرورة رفع وعي الشباب الجامعي وتثقيفهم بظاهرة الابتزاز الالكتروني.
4. قد تُساهم نتائج الدراسة في إثراء الجانب النظري لطريقة خدمة الجماعة في مجال تكنولوجيا المعلومات والاتصال، وخصوصًا في مجال الابتزاز الالكتروني.
5. قد تُفيد نتائج الدراسة الاخصائيين الاجتماعيين في تحسين تدخلهم المهني مع الطلاب المتضررين من ظاهرة الابتزاز الالكتروني، بالاضافة الي تصميم برامج توعية وتثقيف أكثر فعالية، بما يعزز من سلامة ورفاهية الطلاب في بيئة الجامعة.

ثالثا : أهداف الدراسة:

يتحدد الهدف الرئيس للدراسة في" تحديد مستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ".

وينبثق من هذا الهدف الرئيس الأهداف الفرعية التالية:

1. تحديد مستوي معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني.
2. تحديد مستوي اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني.
3. تحديد مستوي الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني.
4. التوصل إلي سبل مقترحة من منظور طريقة خدمة الجماعة لمواجهة ظاهرة الابتزاز الالكتروني لدي طلبة الجامعة.

رابعا: تساؤلات الدراسة:

يتحدد التساؤل الرئيس للدراسة في" ما مستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني؟"

وينبثق من هذا التساؤل الرئيس التساؤلات الفرعية التالية:

1. ما مستوي معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني؟
2. ما مستوي اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني؟
3. ما مستوي الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني؟

خامسا : مفاهيم الدراسة : تتناول الدراسة المفاهيم التالية

(1) مفهوم الابتزاز الالكتروني

الابتزاز

يُعرف الابتزاز من الناحية اللغوية وفقًا لقاموس المعاني بأنه ينبع من المصدر "ابتز"، حيث يعني استخدام القوة أو التهديد للحصول على المال من الآخرين بطرق غير قانونية، مثل سلبهم إياه بشكل جبري وقهري. ويمكن أيضًا أن يُشير إلى استخدام الحيل والخداع لاستدراج الآخرين والحصول على مكاسب غير مشروعة. على سبيل المثال، يمكن أن يكون المبتز شخصًا محتالًا يهدد جيرانه بأفعال ضارة إذا لم يتبعوا تعليماته . (النوفلي واللويهية، 2019، ص21)

وفي معجم لسان العرب، يُعرف الابتزاز في اللغة بأنه كلمة مشتقة من المصدر الثلاثي "بزز"، وتعني سلب الشيء بالقوة بدون وجه حق. وعندما نقول "ابتززت الشيء"، فإننا نعني سلبه بطريقة غير مشروعة. والسلب هو الأخذ بالقوة بدون مبرر قانوني ، أما في الاصطلاح، فإن الابتزاز يشير إلى محاولة سلب إرادة وحرية شخص ما، من خلال إلحاق الأذى النفسي والجسدي به، بهدف تحقيق مكاسب مادية أو غايات غير أخلاقية. (الشكيلية، 2019، ص 25)

والابتزاز الإلكتروني يُعَدُّ إحدى صور الجرائم الإلكترونية (Cyber-crimes)، حيث يتألف مصطلحه من مقطعين: الجريمة (Crime)، والمقطع الآخر (Cyber) الذي يُشير إلى الفضاء الإلكتروني. يُستخدم مصطلح الإلكترونية لتوضيح فكرة أن الجريمة تتم عبر التكنولوجيا الحديثة. وتُعَرَّف الجريمة بأنها الأفعال المخالفة للقانون، وتُعتبر الجرائم الإلكترونية "المخالفات التي تُرتكب ضد الأفراد أو المجموعات بدافع الجريمة، بهدف إيذاء سمعة الضحية أو إلحاق أذى مادي أو عقلي مباشر أو غير مباشر، باستخدام شبكات الاتصال عبر الإنترنت، مثل غُرف الدردشة، والبريد الإلكتروني، والهواتف النقالة، والحواسيب الشخصية ، فالابتزاز الإلكتروني هو أسلوب من أساليب الضغط والاكراه يُمارَس على المجني عليه، بهدف الوصول إلى أهداف غير مشروعة، سواء كانت مادية أو معنوية. وفي حال عدم استجابة المجني عليه للجاني، فإن الأخير يلجأ إلى نشر المعلومات السرية على الملأ، مما يضع المجني عليه في مأزق بين الرضوخ للجاني وتحقيق مطالبه، أو تعريض نفسه للفضيحة.(الخالدى، 2020، ص 2056)

ويُعتبر الابتزاز تهديدًا وترهيبًا للضحية، حيث يُهدد بنشر صور أو مواد مسجلة، أو تسريب بيانات شخصية حساسة مقابل دفع مال أو لاستغلال الضحية في أعمال غير قانونية لصالح المبتز. وغالبًا ما يبدأ الابتزاز بإقامة صداقة مع الشخص الهدف، ثم يتطور التواصل عبر وسائل التواصل الاجتماعي، نظرًا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع. بعد ذلك، يُغري المبتز الضحية ويُسجل المحادثة التي تحتوي على محتوى مسيء للضحية، أو يقوم بقرصنة الحسابات الشخصية وإنشاء صور مفبركة. (Mohamed, 2022)

يمكن القول إن الابتزاز الإلكتروني هو محاولة للحصول على مكاسب مادية أو معنوية من قِبل شخص يستخدم وسائل التواصل الاجتماعي، حيث يحاول استغلال الضحية بشكل فظي أو من خلال صور أو مقاطع فيديو مسجلة أو رسائل صوتية، ويهددها بالرضوخ لمطالبه العاطفية أو المالية.(الحسينى، 2023، ص 330)

كما يعتبر الابتزاز الإلكتروني هو استخدام الإمكانيات التكنولوجية الحديثة ضد الضحية، مثل التهديد بنشر معلومات سرية خاصة أو متعلقة بجهة العمل. عادةً ما يتم اصطياد الضحايا عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي المختلفة، نظرًا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع. يقوم الابتزاز بتحصيل المال أو المنافع من الأشخاص تحت التهديد، وتكون المعلومات المستخدمة في عملية الابتزاز محرجة للضحية. وبالتالي، يعتمد سلوك الابتزاز على وجود عدة عناصر أساسية، بما في ذلك المبتز (الفاعل)، والضحية (المتضررة)، ومحل (موضوع) الابتزاز، بالإضافة إلى العملية الرئيسية في الابتزاز وهي التهديد.(أبو زيد، 2002، ص 4) .

يمكن القول إن الابتزاز الالكتروني هو تهديد شخص بفضح أمره أو كشف سره، وحمله على القيام بفعل معين أو الامتناع عنه، باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات. يتميز الابتزاز الالكتروني عن التهديد بتنفيذ المجني عليه لما يطلبه الجاني. فإذا قام المجني عليه بذلك الفعل، سواء كان فعلًا أم امتناعًا عنه، فإن ذلك يُعتبر ابتزازًا وليس مجرد تهديد. ولا يُشترط التكرار لاعتبار الفعل ابتزازًا، بل يكفي قيام المجني عليه بذلك حتى لو حدث مرة واحدة (حسين، 2019، ص 128)، وتعرف المادة (18) من قانون مكافحة جرائم تقنية المعلومات في القانون العماني الابتزاز الالكتروني بأنه استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في تهديد شخص أو ابتزازه لحمله على

القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع عنه مشروعاً. وبذلك، فإن الابتزاز الالكتروني يتضمن عدة عناصر، أهمها عنصر الإكراه والإجبار. يظهر الإكراه في هذا السياق على شكل تهديد الضحية، حيث لا يقترن الجاني بالضحية بشكل ملموس كالأسلحة أو القوة البدنية، بل يضعه تحت وطأة الإكراه المعنوي، الذي يتيح للضحية درجة محدودة من الاختيار ولكن بشكل ضئيل جداً. العنصر الثاني هو أن يكون هناك هدف للابتزاز، يتمثل في حصول الجاني على شيء مقابل فعله، سواء كان ذلك منفعة مادية أو معنوية غير مشروعة. وبالتالي، لا يُعتبر الفعل ابتزازًا إذا كان لمجرد إلحاق الضرر، مثلما يحدث في حالات الانتقام الإباحي وغيرها. العنصر الثالث هو استخدام تقنية المعلومات كجزء من عملية الابتزاز، حيث يصبح الفعل ابتزازاً إلكترونياً فقط عندما يتم ذلك باستخدام وسائل تقنية المعلومات أو الشبكة المعلوماتية. إذا تم ذلك بطرق أخرى، فإنه يُعتبر ابتزازاً في صورته التقليدية (المقبالى، 2019، ص 93)

أنواع الابتزاز: يشتمل الابتزاز على عدة تصنيفات ومنها:

الابتزاز المادي: يشمل محاولة أخذ المال أو الحصول على مكاسب مادية عن طريق إكراه الضحية على الدفع واستغلال ضعفها.

الابتزاز الالكتروني: يتميز هذا النوع بتوظيف الوسائل الإلكترونية لاستغلال واستمالة الضحية، ومن ثم تهديدها بنشر المقاطع المسجلة أو الصور أو المعلومات السرية الخاصة بها، سواء لتحقيق أهداف مادية أو غير أخلاقية (الشكيلية، 2019، ص 53)

الابتزاز العاطفي: يشير إلى السلوك أو الخطاب الذي يستخدمه الابتزاز لجعل الطرف الآخر يشعر بالخجل أو الخطأ، أو جعله يتحمل مسؤولية لا يستطيع تحملها، ويتم استخدامه لتحقيق السيطرة العاطفية والنفسية على الآخرين.

الابتزاز الأخلاقي: يتم من خلال التهديد باستخدام وسائل مجردة مثل استخدام لغة قاسية في التهديد والتعهد بالكشف عن سر الضحية، بغض النظر عن نوعه سواء كان صورًا، أو فيديوهات، وغيرها (Mohamed, 2022)

صفات شخصية الشخص المعرض للابتزاز : (الغديان وآخرون، 2018، ص178)

- الهروب من الواقع والخوف من كل تعاون أو تعامل مع الآخرين. .
- الاستعداد للفشل أكثر من الاستعداد للنجاح رغم الإدعاء أحيانا بحب النجاح.
- الاعتماد على الآخرين، بسبب التقاعس والتسويف.

- عدم وجود هدف للحياة.
- سهولة التأثر بالآخرين، وعدم القدرة على التمييز بين الأمور.

وأكدت على ذلك دراسة الرويس(2020) حيث اشارات الى أن الشخص المعرض للابتزاز يتمتع بشخصية سلبية غير قادرة على حل المشكلات والتكيف مع المحيط الاجتماعي الذي يعيش فيه، كما أنه شخص غير قادر على إنجاز الأعمال والمهام في وقتها، هذا بالإضافة لفقدانه أهدافًا واضحة تساعده على الانتقال إلى واقع أفضل بكثير من واقعه الحالي الذي يعيش فيه.

كيفية وقوع الابتزاز الالكتروني:

غالباً ما يسهم الضحايا في وقوع فعل الابتزاز، حيث يعمل المبتزون على جمع المعلومات عن الضحايا قبل البدء في ارتكاب جريمتهم، من خلال تصفح وسائل التواصل الاجتماعي الخاصة بهم. في المرحلة الثانية، يتم تحديد الهدف.

تختلف طريقة وقوع الابتزاز باختلاف الضحية. إذا كانت الضحية من الشبان، يقوم المبتز بنسج شباكه حول الضحية من خلال انتحال الشخصيات التي يرغب الضحية بالتواصل معها، مثل انتحال شخصية فتاة ترغب في التعرف على الشاب والتواصل معه. ثم يبدأ التواصل بين الجاني والضحية حتى يكسب الجاني ثقة الضحية، ثم ينتقل إلى التواصل بواسطة التطبيقات التي تتيح التواصل المرئي والحصول على المواد المناسبة للاستغلال مثل الصور ومقاطع الفيديو.

في المرحلة الأخيرة، يكشف المبتز عن شخصيته الحقيقية، ويطالب الضحية بما يريد فوراً، حتى يعطل قدرتها على التفكير في حل مشكلتها، في مقابل عدم نشر المواد المستغلة في الابتزاز. أما إذا كانت الضحية فتاة، فإن وقوع الابتزاز يختلف في الطريقة، حيث يقوم الجاني بالتلطف مباشرة للضحية حتى يتم التواصل عبر وسائل تقنية المعلومات، ثم تتعمق العلاقة حتى يحقق الجاني هدفه (المقبالى، 2019، ص 94)

مخاطر الابتزاز الالكتروني

هناك مخاطر وعواقب متعددة لجريمة الابتزاز الالكتروني ومنها : (Mohamed, 2022)

- **المخاطر الاجتماعية:** انتشار جرائم الابتزاز يعتبر انتهاكًا للسلم المدني، حيث يشكل خطرًا وتهديدًا للفرد والعائلة وبالتالي المجتمع. قد يتردد الشباب والفتيات عن الزواج بسبب الأسرار التي كشفها الابتزاز أمام المجتمع. وأصبح الظلم والقهر أمورًا شائعة أيضًا بسبب صعوبات التعامل مع الآخرين والرغبة في

الانتقام من الجاني ومن الذات، بالإضافة إلى انخفاض تقدير الذات وسيطرة الأفكار غير المنطقية وعدم القدرة على التركيز والاستقرار.

- **المخاطر الأمنية :** جرائم الابتزاز تؤدي إلى اضطراب في الأمن والسلامة في المجتمعات، حيث لا يشعر الأفراد بالأمان لأنفسهم وأسرهم. الأمان والسلامة يعتبران من أهم المعايير لتقييم سلامة المجتمع، ووجود مثل هذه الجرائم يؤدي إلى انهيار هوية المجتمع واضطرابه، مما يساهم في انتشار الفساد.
- **المخاطر النفسية :** تظهر مخاطر الابتزاز في تأثيرات نفسية ترافق الضحية طوال حياته، وقد تتطور لتجعل استمرار حياته مستحيلاً، مما يجعله يفقد الثقة في الآخرين ويصبح شخصية مضطربة وغير طبيعية، وقد تؤدي إلى الاكتئاب والانهيار العصبي والقلق المزمن. يؤثر الابتزاز أيضًا على العائلة بشكل عام، حيث يعانون من أمراض واضطرابات عقلية.

كما اشارت دراسة المقبالى، (2019) الي انه يترتب على الابتزاز الالكتروني مجموعة من المخاطر والعواقب ومنها :

- إدخال الضحايا في دوامة الديون والمشكلات المالية.
- انهيار الأسر عند اكتشاف أفعال الضحايا.
- تضطر الضحايا إلى ارتكاب الجرائم إما لتوفير الأموال المطلوبة أو للرضوخ للمبتزين.
- تعرض الضحايا للاضطرابات النفسية.
- الانتحار.

كيفية تجنب الابتزاز الالكتروني:

يمكن تجنب الابتزاز الالكتروني باتباع مجموعة من النقاط عند استخدام وسائل تقنية المعلومات، ومنها ما اشارت اليها دراسة **المقبالى، (2019)** مثل:

- احترام الشريعة الإسلامية في استخدام هذه الوسائل، فالمبتزون يبحثون عن ما يخشى الضحية اكتشافه، وهذا مطلب لا يتحقق إلا إذا خرج فعل الضحية عن الشريعة الإسلامية.
- المحافظة على البيانات الشخصية، وعدم نشرها في وسائل التواصل الاجتماعي حتى لا تصبح متاحة للمتربصين بها.

- عدم الخوف من المبتزين؛ لأن ذلك يزيد من قوة المبتز، ويفاقم المشكلة، بل يجب التفكير بحكمة في اختيار الحل المناسب والتواصل مع من يمكنه المساعدة.
- التواصل مع المواقع التي نشرت عليها مادة الابتزاز، فالمواقع الالكترونية تتيح التواصل معها وتقديم الشكاوى حول المخالفات التي تقع من مستخدمي الموقع، وعدم الرضوخ للمبتزين، فذلك ليس حلاً للمشكلة، بل يفاقم الضرر، فمن يدفع المال إلى المبتز يستمر في طلب المال.

هذا ويمكن للباحثان تحديد المقصود بالابتزاز الالكتروني في إطار الدراسة الحالية بأنه:

- سلوك إجرامي يعتمد على استخدام وسائل التكنولوجيا الحديثة، مثل الإنترنت أو الهواتف الذكية، بهدف ابتزاز الضحية وإلحاق الضرر بها.
- يستغل هذا السلوك نقاط ضعف الضحية وينتهك خصوصيتها، مستخدمًا أساليب متعددة مثل إرسال رسائل تهديد أو بريد إلكتروني، أو نشر صور أو مقاطع فيديو محرجة على الإنترنت.
- يتسبب هذا السلوك بضرر جسيم لطلبة الجامعة على مختلف الأصعدة (عاطفيًا، ماديًا، جنسيًا، اجتماعيًا، اقتصاديًا، ...الخ).
- يتطلب هذا السلوك الخطير رفع مستوى الوعي بظاهرة الابتزاز الالكتروني بين طلبة الجامعة.

سادسا : المنطلقات النظرية للدراسة

نظرية المخالطة الفارقة

هي إحدى النظريات الاجتماعية التي تشرح السلوك الاجتماعي، والتي يمكنها أن تساهم في فهم وتفسير ظاهرة الابتزاز الإلكتروني ، حيث تشير هذه النظرية إلى أن السلوك الإجرامي، مثل أي نوع آخر من السلوك، قابل للتعلم والانتقال من خلال تفاعل الأفراد ومختلف البيئات الاجتماعية ، فعلى سبيل المثال، تلعب جماعات الأصدقاء دورًا مهمًا في تأثير بعضها البعض لممارسة الجريمة، ويسهل استخدام مواقع التواصل الاجتماعي وتطبيقات الدردشة والألعاب الإلكترونية انتشار هذا السلوك، مثل سناب شات وتويتر والإنستقرام، حيث يستخدم الأشخاص الحسابات الوهمية لأغراض مختلفة، مثل زيادة عدد المتابعين أو الابتزاز أو التشويه والإساءة إلى السمعة ، وتعمل هذه الجماعات الوهمية على ظهور جرائم الابتزاز الإلكتروني نتيجة لمخالطة الأفراد في البيئات المختلفة، سواء في الحياة الواقعية أو عبر الإنترنت. يجمع الأفراد هذه المجموعات

لأهداف مشتركة في بيئات اجتماعية تشجع على التفاعل وتبادل الأفكار، مما يؤدي إلى انتشار الأفكار غير المرغوبة مثل الابتزاز الإلكتروني بشكل مباشر ومستمر. (الحربي وسليمان، 2022، ص 7)

ونقطة البدء في نظرية المخالطة الفارقة (أو كما يسميها البعض بنظرية الجماعات المتباينة) هي رفض التفسير العضوي (البيولوجي) للسلوك الإجرامي. فالجريمة الالكترونية ليست سلوكًا موروثًا، بل سلوك مكتسب. ويتحقق هذا الاكتساب عن طريق مجموعة من التفاعلات الشخصية داخل جماعة محدودة من الأفراد وثيقة الأواصر (نوال ومحمد، 2022، ص 679). لذلك، فنظرية المخالطة الفارقة قائمة على أنّ السلوك يكتسب من خلال التعلم ومخالطة الجماعة. وحيثما توجد الفرصة، توجد الرغبة عند الفرد أو الجماعة لانتقال هذا السلوك، سواء كان سيئًا أو غير سيئ.

وتقوم نظرية المخالطة الفارقة على مجموعة قواعد أو مبادئ أساسية، منها: (فريجة وهياق ، 2019 ، ص 124)

1. يُكتسب السلوك الإجرامي عن طريق التعلم: فهو ليس سلوكًا فطريًا. بمعنى آخر، لا يمكن للشخص الذي لم يتدرب على الجريمة أن يرتكب فعالًا إجراميًا.
2. يُكتسب السلوك الإجرامي عن طريق التعلم المتصل بأشخاص آخرين تربطهم بالشخص عملية اتصال مباشر. تتميز هذه العملية بأنها لفظية في معظم جوانبها، في نفس الوقت الذي تنطوي فيه على الاتصال عن طريق الإشارة.

كما تشير نظرية المخالطة الفارقة إلى تأثير قوة الجماعة على الفرد، وكيف تكسبه سلوكها بطريقة غير مباشرة وغير مقصودة. فمن خلال التفاعل مع الآخرين، يبدأ الفرد بتبني أفكارهم وقيمهم، ممّا قد يؤدي إلى تغيّر سلوكه بشكل تدريجي دون وعي أو قصد مباشر (نوال ومحمد ، 2022، ص 681). وفي سياق الابتزاز الإلكتروني، تعتبر نظرية المخالطة الفارقة ذات أهمية كبيرة. فمن خلال الاختلاط بأشخاص يميلون إلى هذا النوع من السلوك، قد يُصبح الفرد عرضة للتأثر بأفكارهم وقيمهم، ممّا قد يدفعه إلى ارتكاب جرائم ابتزاز إلكتروني .

كما نجد أنّ العلاقة بين نظرية المخالطة الفارقة وجرائم الابتزاز الإلكتروني تظهر من خلال اعتماد النظرية على فكرة أنّ السلوك الإجرامي ينمو وينتقل من خلال التفاعل والتخاطب مع الآخرين. ويمثل هذا التفاعل أساس جريمة الابتزاز الإلكتروني، حيث لا يمكن حدوث العملية إلا بتوافر عملية التواصل بين المبتز والشخص المستهدف من الجريمة من جهة أخرى.

سابعا : الإجراءات المنهجية للدراسة:

(1) نوع الدراسة ومنهجيتها:

تعد هذه الدراسة من الدراسات الوصفية التي لديها القدرة على تقديم التفسيرات العلمية والمنطقية للظاهرة محل الدراسة، وكذلك فالدراسات الوصفية من أنسب أنواع الدراسات لموضوع الدراسة الراهنة حيث أنها تركز علي رصد وتحليل واقع وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني وصولاً إلى سبل مقترحة لمواجهتها من منظور طريقة خدمة الجماعة. واعتمدت الدراسة على استخدام المسح الاجتماعي بطريقة العينة لطلبة مجموعة العمل الاجتماعي بقسم العلوم الاجتماعية كلية الآداب والعلوم التطبيقية جامعة ظفار بسلطنة عمان بالعام الأكاديمي 2024/2023م وعددهم (60) مفردة.

(2) مجالات الدراسة:

(أ) **المجال المكاني:** تمثل المجال المكاني للدراسة في كلية الآداب والعلوم التطبيقية جامعة ظفار بسلطنة عمان.

(ب) المجال البشري: يتكون مجتمع الدراسة من جميع طلبة مجموعة العمل الاجتماعي بقسم العلوم الاجتماعية في كلية الآداب والعلوم التطبيقية بجامعة ظفار في سلطنة عمان، خلال العام الأكاديمي 2024/2023م. ويبلغ عددهم الإجمالي 85 طالبًا وطالبة.

عينة الدراسة:

تم اختيار عينة عشوائية من مجتمع الدراسة مكونة من 60 طالبًا وطالبة. تم اختيار هذه العينة لضمان تمثيلها لجميع أعضاء مجتمع الدراسة من حيث الخصائص الديموغرافية والاهتمامات والأنشطة، بالإضافة إلى عدد (10) مفردات لإجراء اختبارات الصدق والثبات.

(ج) المجال الزمني: تمثل المجال الزمني للدراسة في فترة جمع البيانات من الميدان والتي بدأت من 22 نوفمبر 2023 إلى 22 ديسمبر 2023م.

(3) أبعاد الدراسة ومصادرها:

الأبعاد الرئيسة	الأبعاد الفرعية	عدد العبارات
وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني	معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني	10
	اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني	10
	الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني	10
وتحددت أهم مصادر تلك المتغيرات في: الرجوع إلى الأدبيات النظرية الموجهة للدراسة والدراسات السابقة المرتبطة بالقضية البحثية للدراسة.		

(4) أدوات الدراسة: تمثلت أدوات جمع البيانات في: استمارة استبيان للطلبة حول وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني:

1. قام الباحثان بتصميم استبيان الكتروني للطلبة باستخدام Google Drive Models حول وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني اعتماداً على الأدبيات النظرية الموجهة للدراسة والدراسات السابقة المرتبطة بالقضية البحثية للدراسة.
2. اشتملت استمارة استبيان الطلبة على المحاور التالية: البيانات الأولية، وأبعاد وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني.
3. اعتمدت استمارة استبيان الطلبة على التدرج الثلاثي، بحيث تكون الاستجابة لكل عبارة (نعم، إلى حد ما، لا) وأعطيت لكل استجابة من هذه الاستجابات وزناً (درجة)، **وذلك كما يلي:**

جدول رقم (1) يوضح درجات استمارة استبيان الطلبة

الاستجابات	نعم	إلى حد ما	لا
الدرجة	3	2	1

4. **تحديد مستوى أبعاد استمارة استبيان الطلبة:**

يمكن تحديد مستوى أبعاد استمارة استبيان الطلبة باستخدام المتوسط الحسابي حيث تم ترميز وإدخال البيانات إلى الحاسب الآلي، ولتحديد طول خلايا المقياس الثلاثي (الحدود الدنيا والعليا)، تم حساب المدى = أكبر قيمة – أقل قيمة (3–1 = 2)، تم تقسيمه على عدد خلايا المقياس للحصول على طول الخلية المصحح (3/2 = 0.67) وبعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس أو بداية المقياس وهى الواحد الصحيح وذلك لتحديد الحد الأعلى لهذه الخلية، **وهكذا أصبح طول الخلايا كما يلي:**

جدول رقم (2) يوضح مستويات أبعاد استمارة استبيان الطلبة

القيم	المستوى
إذا تراوحت قيمة المتوسط للعبارة أو البعد من 1 إلى 1.67	مستوى منخفض
إذا تراوحت قيمة المتوسط للعبارة أو البعد من 1.68 إلى 2.34	مستوى متوسط
إذا تراوحت قيمة المتوسط للعبارة أو البعد من 2.35 إلى 3	مستوى مرتفع

5. صدق الأداة:

(أ) **صدق المحتوى** " **الصدق المنطقي** ": للتحقق من صدق المحتوى " الصدق المنطقي " لاستمارة استبيان الطلبة، **قام الباحثان بما يلي:**

- الإطلاع علي الأدبيات والكتب، والأطر النظرية، والدراسات والبحوث السابقة التي تناولت أبعاد الدراسة.
- ثم تحليل هذه الأدبيات النظرية وذلك للوصول إلي الأبعاد المختلفة والعبارات المرتبطة بهذه الأبعاد ذات الارتباط بمشكلة الدراسة، وذلك لتحديد أبعاد وعي طلبة الجامعة بمخاطر الابتزاز الالكتروني والمتمثلة في (معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني، واتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني، والممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني).
- ثم تم عرض الأداة على عدد (3) محكمين من أعضاء هيئة التدريس بكلية الآداب والعلوم التطبيقية – جامعة ظفار بسلطنة عمان لإبداء الرأي في صلاحية الأداة من حيث السلامة اللغوية للعبارات من ناحية وارتباطها بأبعاد الدراسة من ناحية أخرى، وقد تم تعديل وإضافة وحذف بعض العبارات وإعادة تصحيح بعض أخطاء الصياغة اللغوية للبعض الأخر، وبناء على ذلك تم صياغة الأداة في صورته النهائية.

(ب) صدق الاتساق الداخلي:

اعتمد الباحثان في حساب صدق الاتساق الداخلي لاستمارة استبيان الطلبة على معامل ارتباط كل بعد في الأداة بالدرجة الكلية للأداة، وذلك بتطبيقه على عينة قوامها (10) مفردات من الطلبة مجتمع الدراسة، وتبين أنها معنوية عند مستويات الدلالة المتعارف عليها، وأن معامل الصدق مقبول، **وذلك كما يلي:**

جدول رقم (3) يوضح الاتساق الداخلي بين أبعاد استمارة استبيان الطلبة ودرجة الأداة ككل (ن=10)

الأبعاد	المعرفة	الاتجاهات	الممارسات الفعلية
قيمة المعامل	0.972	0.919	0.960
الدلالة	**	**	**

** معنوي عند (0.01) * معنوي عند (0.05)

يوضح الجدول السابق أن:

توجد علاقة طردية دالة إحصائياً عند مستوى معنوية (0.01) بين أبعاد استمارة استبيان الطلبة، ومن ثم تحقق مستوى الثقة في الأداة والاعتماد على نتائجها.

6. **ثبات الأداة:** تم حساب ثبات استمارة استبيان الطلبة باستخدام معامل ثبات (ألفا كرونباخ) لقيم الثبات التقديرية، وذلك بتطبيقه على عينة قوامها (10) مفردات من الطلبة مجتمع الدراسة، وتبين أن معاملات الثبات للأبعاد تتمتع بدرجة عالية من الثبات، **وذلك كما يلي:**

جدول رقم (4) يوضح نتائج ثبات استمارة استبيان الطلبة (ن=10)

الأبعاد	المعرفة	الاتجاهات	الممارسات الفعلية	ثبات الأداة ككل
معامل (ألفا - كرونباخ)	0.897	0.855	0.909	0.942

يوضح الجدول السابق أن:

معاملات الثبات لأبعاد استمارة استبيان الطلبة تتمتع بدرجة عالية من الثبات والدقة والموثوقية، وأصبحت الأداة في صورتها النهائية، وبذلك يمكن الاعتماد على نتائجها، كما أن نتائجها قابلة للتعميم على مجتمع الدراسة.

(5) أساليب التحليل الكيفي والكمي:

اعتمدت الدراسة في تحليل البيانات على الأساليب التالية:

- **أسلوب التحليل الكيفي:** بما يتناسب وطبيعة موضوع الدراسة.
- **أسلوب التحليل الكمي:** تم معالجة البيانات من خلال الحاسب الآلي باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS.V. 24.0)، وقد طبقت الأساليب الإحصائية التالية: التكرارات والنسب المئوية، والمتوسط الحسابي، والانحراف المعياري، والمدى، ومعامل ثبات (ألفا كرونباخ) لقيم الثبات التقديرية، ومعامل ارتباط بيرسون، واختبار (ت) لعينتين مستقلتين، وتحليل التباين أحادي الاتجاه، وطريقة الفرق المعنوي الأصغر لتحديد اتجاه التباين لصالح أي مجموعة من المجموعات.

ثامناً: نتائج الدراسة الميدانية:

المحور الأول: وصف الطلبة مجتمع الدراسة:

جدول رقم (5) يوضح وصف الطلبة مجتمع الدراسة (ن=60)

م	النوع	ك	%	م	الحالة الاجتماعية	ك	%
1	ذكر	32	53.3	1	أعزب	58	96.7
2	أنثى	28	46.7	2	متزوج	2	3.3
المجمــوع		60	100	المجمــوع		60	100
م	السن	ك	%	م	المرحلة الأكاديمية	ك	%
1	من 18 لأقل من 20 سنة	8	13.3	1	السنة الأولي	36	60
2	من 20 لأقل من 22 سنة	24	40	2	السنة الثانية	8	13.3
3	من 22 سنة فأكثر	28	46.7	3	السنة الثالثة	9	15
المجمــوع		60	100	4	السنة الرابعة	7	11.7
المتوسط الحسابي		22					
الانحراف المعياري		1		المجمــوع		60	100

يوضح الجدول السابق أن:

-أكبر نسبة من الطلبة ذكور بنسبة (53.3%)، بينما الإناث بنسبة (46.7%).

-أكبر نسبة من الطلبة في الفئة العمرية (من 22 سنة فأكثر) بنسبة (46.7%)، يليها الفئة العمرية (من 20 لأقل من 22 سنة) بنسبة (40%)، وأخيراً الفئة العمرية (من 18 لأقل من 20 سنة) بنسبة (13.3%). ومتوسط سن الطلبة (22) سنة، وبانحراف معياري سنة واحدة تقريباً.

-أكبر نسبة من الطلبة حالتهم الاجتماعية أعزب بنسبة (96.7%)، يليه متزوج بنسبة (3.3%).

-أكبر نسبة من الطلبة بالسنة الأولى بنسبة (60%)، يليها السنة الثالثة بنسبة (15%)، ثم السنة الثانية بنسبة (13.3%)، وأخيراً السنة الرابعة بنسبة (11.7%).

المحور الثاني: أبعاد وعي طلبة الجامعة بمخاطر الابتزاز الالكتروني:

(1) معرفة طلبة الجامعة بمخاطر الابتزاز الالكتروني:

جدول رقم (6) يوضح معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني (ن=60)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
1	معرفة طلبة الجامعة بأن الابتزاز الالكتروني هو نوع من الجرائم التي يتم فيها استخدام الانترنت أو أي وسيلة إلكترونية أخرى للتهديد أو الضغط على شخص ما للحصول على شيء منه، مثل المال أو المعلومات أو القيام بأمر ما	47	78.3	12	20	1	1.7	2.77	0.46	4
2	الابتزاز الالكتروني يمكن أن يكون باستخدام الصور أو الفيديوهات الشخصية للضحية، والتي قد تكون تم التقاطها دون علم أو موافقة الضحية	48	80	12	20	-	-	2.8	0.4	3
3	الابتزاز الالكتروني يمكن أن يكون باستخدام معلومات شخصية أو مالية للضحية، مثل رقم الهاتف أو عنوان البريد الالكتروني أو بيانات بطاقة الائتمان	49	81.7	8	13.3	3	5	2.77	0.53	5
4	الابتزاز الالكتروني يمكن أن يكون بطلب إنجاز أعمال غير قانونية من الضحية، مثل نشر معلومات مضللة أو سرقة بيانات شخصية	45	75	13	21.7	2	3.3	2.72	0.52	8
5	الابتزاز الالكتروني يمكن أن يحدث عبر مجموعة متنوعة من المنصات الالكترونية، مثل وسائل التواصل الاجتماعي والتطبيقات وخدمات البريد الالكتروني	45	75	15	25	-	-	2.75	0.44	6
6	الابتزاز الالكتروني يمكن أن يسبب مشاكل نفسية واجتماعية للضحية، مثل القلق والاكتئاب والخوف من التعرض للخطر	49	81.7	11	18.3	-	-	2.82	0.39	2
7	الابتزاز الالكتروني هو جريمة يعاقب عليها القانون في العديد من الدول	51	85	9	15	-	-	2.85	0.36	1
8	هناك العديد من الطرق التي يمكن من خلالها الوقاية من الابتزاز الالكتروني مثل عدم نشر أي معلومات شخصية على الانترنت	46	76.7	12	20	2	3.3	2.73	0.52	7

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
9	معرفة الطلبة الجامعيين بأهمية حفظ الأدلة في حالة تعرضهم للابتزاز الالكتروني، فهذه الأدلة قد تساعدهم على مقاضاته	48	80	12	20	-	-	2.8	0.4	3
10	معرفة الجهات التي يمكن اللجوء إليها للحصول على الدعم والمساعدة في حالة التعرض للابتزاز الالكتروني كالشرطة أو مراكز مكافحة الابتزاز الالكتروني	45	75	15	25	-	-	2.75	0.44	6
	المعرفة ككل							2.78	0.31	مستوى مرتفع

يوضح الجدول السابق أن:

مستوى **معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني** مرتفع حيث بلغ المتوسط الحسابي (2.78)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: الترتيب الأول الابتزاز الالكتروني هو جريمة يعاقب عليها القانون في العديد من الدول بمتوسط حسابي (2.85)، يليه الترتيب الثاني الابتزاز الالكتروني يمكن أن يسبب مشاكل نفسية واجتماعية للضحية، مثل القلق والاكتئاب والخوف من التعرض للخطر بمتوسط حسابي (2.82)، ثم الترتيب الثالث الابتزاز الالكتروني يمكن أن يكون باستخدام الصور أو الفيديوهات الشخصية للضحية، والتي قد تكون تم التقاطها دون علم أو موافقة الضحية، ومعرفة الطلبة الجامعيين بأهمية حفظ الأدلة في حالة تعرضهم للابتزاز الالكتروني، فهذه الأدلة قد تساعدهم على مقاضاته بمتوسط حسابي (2.8)، وأخيراً الترتيب الثامن الابتزاز الالكتروني يمكن أن يكون بطلب إنجاز أعمال غير قانونية من الضحية، مثل نشر معلومات مضللة أو سرقة بيانات شخصية بمتوسط حسابي (2.72)، ويتفق هذا مع ما أوضحته دراسة (حسين، 2019، ص 128)، التي وصفت الابتزاز الإلكتروني على أنه حمل شخص على القيام بفعل أو الامتناع عنه، بعد تهديده باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات. ويتماشى هذا أيضًا مع دراسة (Mohamed، 2022)، التي أشارت إلى أن الابتزاز الإلكتروني يهدف إلى تهديد وترهيب الضحية بنشر صور أو مواد مسجلة أو تسريب بيانات شخصية. كما أشارت دراسة (الحسيني، 2023، ص 330) إلى أن الابتزاز الإلكتروني يهدف إلى حصول الشخص على مكاسب مادية أو

معنوية، واستمالة الضحية لفظيًا أو بالصور أو بمقاطع الفيديو المسجلة، وتهديدها للرضوخ بمطالب الجاني العاطفية أو المالية ، كما يتفق ذلك مع ما اشارت اليه نظرية المخالطة الفارقة من اهمية التواصل في انتشار السلوكيات والجرائم بما في ذلك الابتزاز الالكتروني الذي يعتمد علي التواصل بين المبتز والضحية .

(2) اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني:

جدول رقم (7) يوضح اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني (ن=60)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
1	إيمان طلبة الجامعة بأن الابتزاز الالكتروني ظاهرة خطيرة	53	88.3	7	11.7	-	-	2.88	0.32	2
2	استعداد طلبة الجامعة للإبلاغ عن حالات الابتزاز الالكتروني إلى السلطات المختصة	46	76.7	14	23.3	-	-	2.77	0.43	6
3	استعداد طلبة الجامعة لمناقشة مخاطر الابتزاز الالكتروني مع الآخرين	48	80	11	18.3	1	1.7	2.78	0.45	5
4	رفض طلبة الجامعة الانصياع للمطالب الابتزازية	29	48.3	24	40	7	11.7	2.37	0.69	7
5	استعداد طلبة الجامعة لتقديم الدعم للضحايا الذين تعرضوا للابتزاز الالكتروني	48	80	11	18.3	1	1.7	2.78	0.45	5
6	استعداد طلبة الجامعة للمساهمة في تعزيز التوعية بمخاطر الابتزاز الالكتروني	49	81.7	11	18.3	-	-	2.82	0.39	3
7	مطالبة طلبة الجامعة بسن قوانين أكثر صرامة للتصدي لظاهرة الابتزاز الالكتروني	49	81.7	11	18.3	-	-	2.82	0.39	3
8	استعداد طلبة الجامعة للمشاركة في الأنشطة التوعوية حول مخاطر الابتزاز الالكتروني	50	83.3	9	15	1	1.7	2.82	0.43	4
9	رغبة طلبة الجامعة في تقديم النصائح والمساعدة للضحايا الذين تعرضوا للابتزاز الالكتروني	49	81.7	11	18.3	-	-	2.82	0.39	3
10	عمل طلبة الجامعة على حماية أنفسهم من الابتزاز الالكتروني	54	90	6	10	-	-	2.9	0.3	1
	الاتجاهات ككل							2.78	0.28	مستوى مرتفع

يوضح الجدول السابق أن:

مستوى **اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني** مرتفع حيث بلغ المتوسط الحسابي (2.78)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: الترتيب الأول عمل طلبة الجامعة على حماية أنفسهم من الابتزاز الالكتروني بمتوسط حسابي (2.9)، يليه الترتيب الثاني إيمان طلبة الجامعة بأن الابتزاز الالكتروني ظاهرة خطيرة بمتوسط حسابي (2.88)، ثم الترتيب الثالث استعداد طلبة الجامعة للمساهمة في تعزيز التوعية بمخاطر الابتزاز الالكتروني، ومطالبة طلبة الجامعة بسن قوانين أكثر صرامة للتصدي لظاهرة الابتزاز الالكتروني، ورغبة طلبة الجامعة في تقديم النصائح والمساعدة للضحايا الذين تعرضوا للابتزاز الالكتروني بمتوسط حسابي (2.82)، وأخيراً الترتيب السابع رفض طلبة الجامعة الانصياع للمطالب الابتزازية بمتوسط حسابي (2.37)، هذا يتماشى مع دراسة (المقبالي، 2019، ص 101) التي أكدت ضرورة عدم الخوف من المبتزين؛ حيث إن ذلك يزيد من قوتهم ويفاقم المشكلة. بدلاً من ذلك، ينبغي التفكير بحكمة في الحل المناسب والتواصل مع من يمكنه المساعدة، بالإضافة إلى عدم الرضوخ للمبتزين، فهذا ليس حلاً للمشكلة، بل يزيد من تعقيد الأمور. من يدفع المال إلى المبتزين يجعلهم يستمرون في طلب المال بشكل مستمر."

(3) الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني:

جدول رقم (8) يوضح الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني (ن=60)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
1	لا أرسل صوري أو فيديوهاتي الشخصية إلى أي شخص لا أعرفه جيدًا	53	88.3	7	11.7	-	-	2.88	0.32	2
2	لا أستجب للمطالب الابتزازية	51	85	8	13.3	1	1.7	2.83	0.42	6
3	إذا تعرضت للابتزاز الالكتروني، أبلغ الجهات المختصة	53	88.3	6	10	1	1.7	2.87	0.39	4
4	أستخدم كلمات مرور قوية ومختلفة لكل حساب على الانترنت	54	90	5	8.3	1	1.7	2.88	0.37	3
5	لا أشارك معلوماتي الشخصية مع أي شخص لا أعرفه جيدًا	53	88.3	7	11.7	-	-	2.88	0.32	2

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
6	أقوم بتحديث برامج الأمان على أجهزتي الالكترونية بانتظام	55	91.7	5	8.3	-	-	2.92	0.28	1
7	الحرص على عدم فتح المرفقات أو الروابط المشبوهة التي تصلني من أشخاص لا أعرفهم	53	88.3	7	11.7	-	-	2.88	0.32	2
8	أقوم بتأمين حسابي على مواقع التواصل الاجتماعي، مثل تفعيل خاصية التحقق بخطوتين	53	88.3	7	11.7	-	-	2.88	0.32	2
9	أشارك في الأنشطة التوعية بمخاطر الابتزاز الالكتروني التي تنظمها المؤسسات التعليمية أو المجتمعية	48	80	12	20	-	-	2.8	0.4	7
10	أبحث عن المعلومات المتعلقة بمخاطر الابتزاز الالكتروني واطلع عليها باستمرار	50	83.3	10	16.7	-	-	2.83	0.38	5
	الممارسات الفعلية ككل							2.87	0.27	مستوى مرتفع

يوضح الجدول السابق أن:

مستوى **الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني** مرتفع حيث بلغ المتوسط الحسابي (2.87)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: الترتيب الأول أقوم بتحديث برامج الأمان على أجهزتي الالكترونية بانتظام بمتوسط حسابي (2.92)، يليه الترتيب الثاني لا أرسل صوري أو فيديوهاتي الشخصية إلى أي شخص لا أعرفه جيدًا، ولا أشارك معلوماتي الشخصية مع أي شخص لا أعرفه جيدًا، والحرص على عدم فتح المرفقات أو الروابط المشبوهة التي تصلني من أشخاص لا أعرفهم، وأقوم بتأمين حسابي على مواقع التواصل الاجتماعي، مثل تفعيل خاصية التحقق بخطوتين بمتوسط حسابي (2.88) وبانحراف معياري (0.32)، ثم الترتيب الثالث أستخدم كلمات مرور قوية ومختلفة لكل حساب على الانترنت بمتوسط حسابي (2.88) وبانحراف معياري (0.37)، وأخيراً الترتيب السابع أشارك في الأنشطة التوعية بمخاطر الابتزاز الالكتروني التي تنظمها المؤسسات التعليمية أو المجتمعية بمتوسط حسابي (2.8)، وهذا يتفق مع نظرية المخالطة الفارقة التي توضح طبيعة سلوك الابتزاز الإلكتروني كسلوك إجرامي، حيث يُعتبر مثل أي شكل آخر من السلوك يمكن

تعلمه وانتقاله من خلال التفاعل والمخالطة، وخاصةً مع سهولة استخدام وسائل التواصل الاجتماعي وتطبيقات الدردشة والألعاب الإلكترونية وانتشارها، مثل سناب شات أو تويتر أو الإنستغرام، وذلك من خلال حسابات تحمل أسماء غير حقيقية ، ويتماشى هذا مع دراسة (المقبالي، 2019، ص 101) التي أشارت إلى أنه يمكن تجنب الابتزاز الإلكتروني عند اتخاذ مجموعة من الإجراءات عند استخدام وسائل التكنولوجيا مثل المحافظة على البيانات الشخصية وعدم نشرها على وسائل التواصل الاجتماعي لتجنب أن تكون في متناول المتسللين، وعدم التواصل مع الغرباء الذين لا يمكن التعرف على هوياتهم والذين يختبئون وراء الألقاب والمعرفات الإلكترونية. لذا يجب التحقق من هوية أي شخص قبل التواصل معه قدر الإمكان."

- **مستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل:**

جدول رقم (9) يوضح مستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل (ن=60)

م	الأبعاد	المتوسط الحسابي	الانحراف المعياري	المستوى	الترتيب
1	معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني	2.78	0.31	مرتفع	3
2	اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني	2.78	0.28	مرتفع	2
3	الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني	2.87	0.27	مرتفع	1
أبعاد الوعي ككل		2.81	0.26	مستوى مرتفع	

يوضح الجدول السابق أن:

مستوى **وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل** مرتفع حيث بلغ المتوسط الحسابي (2.81)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: الترتيب الأول الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني بمتوسط حسابي (2.87)، يليه الترتيب الثاني اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني بمتوسط حسابي (2.78) وبانحراف معياري (0.28)، وأخيراً الترتيب الثالث معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني بمتوسط حسابي (2.78) وبانحراف معياري (0.31).

المحور الثالث: المصفوفة الارتباطية للعلاقة بين أبعاد وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني:

جدول رقم (10) يوضح المصفوفة الارتباطية للعلاقة بين أبعاد وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني (ن=60)

الأبعاد / الأبعاد	المعرفة	الاتجاهات	الممارسات الفعلية	أبعاد الوعي ككل
المعرفة	1			
الاتجاهات	**0.775	1		
الممارسات الفعلية	**0.737	**0.724	1	
ابعاد الوعي ككل	**0.926	**0.913	**0.894	1

** معنوي عند (0.01) * معنوي عند (0.05)

يوضح الجدول السابق أن:

توجد علاقة طردية دالة إحصائياً عند مستوى معنوية (0.01) بين أبعاد وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني والمتمثلة في (معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني، واتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني، والممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني، وأبعاد وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل). وقد يرجع ذلك إلي وجود ارتباط طردي بين هذه الأبعاد وأنها جاءت معبرة عما تهدف الدراسة إلى تحقيقه.

المحور الرابع: دلالة الفروق المعنوية بين استجابات الطلبة وفقاً للنوع بالنسبة لتحديدهم لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني:

جدول رقم (11) يوضح دلالة الفروق المعنوية بين استجابات الطلبة وفقاً للنوع بالنسبة لتحديدهم لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني (ن=60)

الأبعاد	مجتمع البحث	العدد(ن)	المتوسط الحسابي	الانحراف المعياري	درجات الحرية (df)	قيمة T	الدلالة
المعرفة	ذكور	32	2.73	0.35	58	1.116-	غير دال
	إناث	28	2.82	0.25			
الاتجاهات	ذكور	32	2.75	0.31	58	0.834-	غير دال
	إناث	28	2.81	0.24			
الممارسات العلية	ذكور	32	2.82	0.31	58	1.441-	غير دال
	إناث	28	2.92	0.2			
أبعاد الوعي ككل	ذكور	32	2.77	0.3	58	1.211-	غير دال
	إناث	28	2.85	0.2			

** معنوي عند (0.01) * معنوي عند (0.05)

يوضح الجدول السابق أن:

- لا توجد فروق جوهرية دالة إحصائياً بين استجابات الطلبة الذكور والإناث بالنسبة لتحديدهم لمستوى معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني.
- لا توجد فروق جوهرية دالة إحصائياً بين استجابات الطلبة الذكور والإناث بالنسبة لتحديدهم لمستوى اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني.
- لا توجد فروق جوهرية دالة إحصائياً بين استجابات الطلبة الذكور والإناث بالنسبة لتحديدهم لمستوى الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني.
- لا توجد فروق جوهرية دالة إحصائياً بين استجابات الطلبة الذكور والإناث بالنسبة لتحديدهم لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل.

المحور الخامس: تحليل التباين لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني طبقاً لاستجابات الطلبة وفقاً لفئات السن:

جدول رقم (12) يوضح تحليل التباين لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني طبقاً لاستجابات الطلبة وفقاً لفئات السن (ن=60)

الأبعاد	مصدر التباين	مجموع المربعات	درجات الحرية (df)	متوسط المربعات	قيمة (ف) F ودلالتها	اختبار LSD
المعرفة	بين المجموعات	0.143	2	0.072	0.744	-
	داخل المجموعات	5.489	57	0.096		
	المجموع	5.633	59			
الاتجاهات	بين المجموعات	0.007	2	0.003	0.043	-
	داخل المجموعات	4.566	57	0.080		
	المجموع	4.573	59			
الممارسات الفعلية	بين المجموعات	0.009	2	0.005	0.062	-
	داخل المجموعات	4.204	57	0.074		
	المجموع	4.213	59			
أبعاد الوعي ككل	بين المجموعات	0.024	2	0.012	0.172	-
	داخل المجموعات	3.957	57	0.069		
	المجموع	3.980	59			

** معنوي عند (0.01) * معنوي عند (0.05)

يوضح الجدول السابق أن:

- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً لفئات السن (الفئة العمرية من 18 سنة إلى أقل من 20 سنة / الفئة العمرية من 20 سنة إلى أقل من 22 سنة/ الفئة العمرية من 22 سنة فأكثر) بالنسبة لتحديدهم لمستوى معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني.
- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً لفئات السن (الفئة العمرية من 18 سنة إلى أقل من 20 سنة / الفئة العمرية من 20 سنة إلى أقل من 22 سنة/ الفئة العمرية من 22 سنة فأكثر) بالنسبة لتحديدهم لمستوى اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني.
- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً لفئات السن (الفئة العمرية من 18 سنة إلى أقل من 20 سنة / الفئة العمرية من 20 سنة إلى أقل من 22 سنة/ الفئة العمرية من 22 سنة فأكثر) بالنسبة لتحديدهم لمستوى الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني.
- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً لفئات السن (الفئة العمرية من 18 سنة إلى أقل من 20 سنة / الفئة العمرية من 20 سنة إلى أقل من 22 سنة/ الفئة العمرية من 22 سنة فأكثر) بالنسبة لتحديدهم لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل.

المحور السادس: تحليل التباين لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني طبقاً لاستجابات الطلبة وفقاً للمرحلة الأكاديمية:

جدول رقم (13) يوضح تحليل التباين لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني طبقاً لاستجابات الطلبة وفقاً للمرحلة الأكاديمية (ن=60)

الأبعاد	مصدر التباين	مجموع المربعات	درجات الحرية (df)	متوسط المربعات	قيمة F (ف) ودلالتها	اختبار LSD
المعرفة	بين المجموعات	0.344	3	0.115	1.214	-
	داخل المجموعات	5.289	56	0.094		
	المجموع	5.633	59			
الاتجاهات	بين المجموعات	0.6	3	0.2	*2.821	2 <1 4 –
	داخل المجموعات	3.972	56	0.071		
	المجموع	4.573	59			

الأبعاد	مصدر التباين	مجموع المربعات	درجات الحرية (df)	متوسط المربعات	قيمة F (ف) ودلالتها	اختبار LSD
الممارسات الفعلية	بين المجموعات	0.764	3	0.255	*4.137	2 <1 4 –
	داخل المجموعات	3.449	56	0.062		
	المجموع	4.213	59			
أبعاد الوعي ككل	بين المجموعات	0.51	3	0.17	2.744	-
	داخل المجموعات	3.47	56	0.062		
	المجموع	3.98	59			

** معنوي عند (0.01) * معنوي عند (0.05)

يوضح الجدول السابق أن:

- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً للمرحلة الأكاديمية (السنة الأولي/ السنة الثانية/ السنة الثالثة/ السنة الرابعة) بالنسبة لتحديدهم لمستوى معرفة طلبة الجامعة بظاهرة الابتزاز الالكتروني.
- يوجد تباين دال إحصائياً عند مستوى معنوية (0.05) بين استجابات الطلبة وفقاً للمرحلة الأكاديمية (السنة الأولي/ السنة الثانية/ السنة الثالثة/ السنة الرابعة) بالنسبة لتحديدهم لمستوى اتجاهات طلبة الجامعة نحو ظاهرة الابتزاز الالكتروني. وهذه الفروق لصالح الفئة الأولى التي تقع في فئة (استجابات الطلبة بالسنة الأولى) لتصبح أكثر استجابات الطلبة وفقاً للمرحلة الأكاديمية تحديداً لتلك الأبعاد.
- يوجد تباين دال إحصائياً عند مستوى معنوية (0.05) بين استجابات الطلبة وفقاً للمرحلة الأكاديمية (السنة الأولي/ السنة الثانية/ السنة الثالثة/ السنة الرابعة) بالنسبة لتحديدهم لمستوى الممارسات الفعلية لطلبة الجامعة للتعامل مع ظاهرة الابتزاز الالكتروني. وهذه الفروق لصالح الفئة الأولى التي تقع في فئة (استجابات الطلبة بالسنة الأولى) لتصبح أكثر استجابات الطلبة وفقاً للمرحلة الأكاديمية تحديداً لتلك الأبعاد.
- لا يوجد تباين دال إحصائياً بين استجابات الطلبة وفقاً للمرحلة الأكاديمية (السنة الأولي/ السنة الثانية/ السنة الثالثة/ السنة الرابعة) بالنسبة لتحديدهم لمستوى وعي طلبة الجامعة بظاهرة الابتزاز الالكتروني ككل.

سابعا: الصعوبات التى واجهت الباحثان أثناء تطبيق الدراسة :

- على الرغم من الجهود التي بذلها الباحثان، إلا أنهم واجهوا بعض الصعوبات في جمع البيانات، حيث لم يلتزم جميع أعضاء العينة بملء الاستمارة.

- **السبل المقترحة من منظور طريقة خدمة الجماعة لمواجهة ظاهرة الابتزاز الالكتروني لدي طلبة الجامعة**

فيما يلي مجموعة من السبل المقترحة والتي تعكس دور الاخصائيين الاجتماعيين العاملين مع جماعات الشباب الجامعي في مواجهة ظاهرة الابتزاز الإلكتروني.

1. تشكيل فريق من جماعات الطلبة المتطوعين المهتمين بنشر الوعي حول ظاهرة الابتزاز الإلكتروني، وتدريب أعضاء الفريق بشكل مكثف لتنظيم الحملات التوعوية داخل الجامعة باستخدام مختلف الوسائل.
2. تنظيم حملات توعية على منصات التواصل الاجتماعي للطلاب والمجتمع الجامعي حول ظاهرة الابتزاز الالكتروني وكيفية الوقاية منها.
3. تنفيذ ندوات وورش عمل وبرامج توعية داخل الجامعة حول خطورة الابتزاز الالكتروني وكيفية التعامل معه بطرق صحيحة.
4. تقديم برامج تدريبية للطلاب والموظفين الجامعيين حول كيفية التعرف على والتعامل مع حالات الابتزاز الإلكتروني.
5. تكوين فريق دعم متخصص من مختصين في الخدمة الاجتماعية وعلم النفس والقانون لتقديم الدعم والمساعدة للطلاب المتضررين من ظاهرة الابتزاز الالكتروني .
6. توفير المعلومات والموارد حول الإجراءات القانونية والشرطية للطلاب الذين يواجهون حالات ابتزاز إلكتروني.
7. التعاون مع الجهات المعنية مثل الشرطة والجمعيات الخيرية والمنظمات غير الحكومية لتنظيم حملات توعوية مشتركة ودعوة خبراء من هذه الجهات لتقديم محاضرات وندوات حول ظاهرة الابتزاز الإلكتروني وطرق الوقاية منه.
8. تعزيز التواصل مع الإدارة الجامعية بهدف تبادل المعرفة وتطوير سياسات جامعية لمواجهة الابتزاز الالكتروني.
9. دعوة أعضاء هيئة التدريس الي تخصيص محاضرات أو ورش عمل ضمن المناهج الجامعية لمناقشة ظاهرة الابتزاز الإلكتروني وطرق الوقاية منها .
10. القيام بأبحاث تحليلية حول ظاهرة الابتزاز الإلكتروني في الجامعات وتحليل أسبابها وتأثيراتها على الطلاب والمجتمع الجامعي.

المراجع

(أ) المراجع العربية:

ابراهيم، وسام محمد (2022) . فعالية البرامج الجماعية في توعية الشباب الجامعى بأشكال التحرش الإلكتروني، مجلة دراسات في الخدمة الاجتماعية ، المجلد 60، العدد 1 ، كلية الخدمة الاجتماعية، جامعة حلوان .

أبو زيد، محمد صابر (2022) . إسهامات الخدمة الاجتماعية في الحد من مخاطر الابتزاز الالكتروني للشباب وتصور مقترح من منظور الأزمة في طريقة خدمة الفرد، مجلة القاهرة للخدمة الإجتماعية، عدد 63، القاهرة .

الحجري، هيثم بن هلال بن عامر (2019) . ظاهرة الابتزاز الالكتروني وتأثيرها على المجتمع الرقمي الحديث، بحث منشور ضمن ندوة (الابتزاز الالكتروني بين التوعية والتجريم)، المعهد العالي للقضاء، سلطنة عُمان .

الحربي، وجدان جمعان وسليمان، منال (2022).دور الخدمة الاجتماعية في رفع الوعي المجتمعي بجرائم الابتزاز الالكتروني: دراسة ميدانية على عينة من طالبات كلية الآداب والعلوم الإنسانية جامعة الملك عبد العزيز بمدينة جدة، مجلة العلوم التربوية والاجتماعية، المجلد 1، العدد 13 .

الحسيني، مروه سعد جاد (2023) . الابتزاز الالكتروني للمرأة المصرية دراسة تطبيقية لعينة من مستخدمي الفيس بوك وانستجرام، حوليات آداب عين شمس - المجلد 51، عدد يناير .

الخالدي، عبير نجم عبدالله (2020) . دور الوعي الاجتماعي في مواجهة الابتزاز الالكتروني للمرأة، مجلة كلية التربية، جامعة واسط ، العراق .

الشكيلية، منى بنت سعيد (2019) . آثار الابتزاز الالكتروني على الصحة النفسية للأطفال، بحث منشور ضمن ندوة (الابتزاز الالكتروني بين التوعية والتجريم)، المعهد العالي للقضاء، سلطنة عُمان .

الرويس، فيصل بن عبد الله. (2020). الوعى الاجتماعى بظاهرة الابتزاز الالكتروني لدى الأسرة في المجتمع السعودي : دراسة ميدانية للعوامل والآثار. مجلة كلية الآداب والعلوم الإنسانية، عدد 33، جامعة قناة السويس.

الغديان، سليمان بن عبد الرزاق وآخرون (2018) . صور جرائم الابتزاز الالكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، المجلد 27، العدد 69، كلية الملك فهد الأمنية .

المقبالي، سعيد بن محمد (2019) . الجريمة الالكترونية في القانون العماني، بحث منشور ضمن ندوة (الابتزاز الالكتروني بين التوعية والتجريم)، المعهد العالي للقضاء، سلطنة عُمان

النوفلي، حمود بن خميس بن حمد و اللويهية، أفراح بنت خميس بن عامر : الآثار الاجتماعية للابتزاز الالكتروني دراسة ميدانية على مدارس الحلقة الثانية بمحافظة جنوب الباطنة، بحث منشور ضمن ندوة (الابتزاز الالكتروني بين التوعية والتجريم)، المعهد العالي للقضاء، الثلاثاء 30 من أبريل ٢٠١٩ م سلطنة عُمان

باطويح، محمد عمر (2010) . جدوى إنشاء إدارة للمخاطر في الشركات االستثمارية، مكتبة آفاق، غرفة تجارة وصناعة الكويت .

حسين، حمدي محمد محمود (2019) . المواجهة التشريعية لجرائم التهديد والابتزاز الالكتروني دراسة تحليلية تأصيلية لموقف المشرع العماني، بحث منشور ضمن ندوة (الابتزاز الالكتروني بين التوعية والتجريم)، المعهد العالي للقضاء، سلطنة عُمان

حنون، هند علي (2023) . وسائل حماية الأسرة من الابتزاز الالكتروني، مجلة جامعة دهوك، المجلد : 26، العدد : 1 (العلوم الانسانية والاجتماعية)، (عدد (خاص)

شعيبث، سلام عبد والسعدي، نور علي (2023) . الحماية الجنائية للمرأة من ظاهرة الابتزاز الالكتروني، مجلة العلوم الانسانية والاجتماعية، جامعة دهوك، المجلد 1، (عدد (خاص).

فريجة ، احمد وهياق ، ابراهيم (2019) . النظريات المفسرة للسلوك الانحرافي والاجرامي ، رؤية اجتماعية ، مجلة تطوير العلوم الاجتماعية ، مجلد 12 ، الجزائر، ص 124)

موسى، عماد جواد (2022) . التحقيق والصعوبات التي تواجه جريمة الابتزاز الالكتروني، مجلة كلية المعارف الجامعة، جامعة الأنبار، الرمادي، العراق، المجلد 33 - العدد 4 .

نوال ، قادة بن عبد الله ومحمد ، حمو (2022) . الجريمة الالكترونية قراءة سوسيولوجية لأهم النظريات المفسرة للسلوك الاجرامي ، مجلة روافد للدراسات والابحاث العلمية في العلوم الاجتماعية والانسانية ، مجلد 6 ، الجزائر

وزارة المالية . (2022). نشرة ادارة المخاطر، الرقابة المالية، العدد 6، المملكة العربية السعودية.

(ب) المراجع الاجنبية:

Chantal, Faucher., Margaret, Jackson., Wanda, Cassidy. (2014). Cyberbullying among University Students: Gendered Experiences, Impacts, and Perspectives. Education Research International, Publishing Corporation، Education Research International.

Chin-Ling, Chen., Jinn-Ke, Jan., Ming-He, Liu. (2007). A traceable E-cash transfer system against blackmail on mobile phones. 1-4. doi: 10.1109/TENCON.2007.4429006

Chin-Ling, Chen., Ming-He, Liu. (2011). A novel and low-computation e-cash transfer system against blackmail for mobile communications. International Journal of Mobile Communications, doi: 10.1504/IJMC.2011.040144

Mohamed, Mekkawi. (2022). Cyber Blackmail between Threats and Protection: A Study of the Egyptian and American Legislations, Journal of Law and Emerging Technologies، issued by the Faculty of Law at the British University in Egypt Volume 02, Issue 02.

Mohammed Salem Alneyadi, Mohammad Amin Alkrisheh, Nour Hamad Alhajaya, Khawlah M. AL-Tkhayneh .(2022) The Crime of Electronic Blackmail in the Emirati Law، International Arab Conference on Information Technology (ACIT) is an academic conference.

Roderic, Broadhurst., Katie, Skinner., Nicholas, Sifniotis., Bryan, Matamoros-Macias., Yuguang, Ipsen. (2020). Phishing risks in a university student community. Social Science Research Network ،Australian Institute of Criminology, Trends & issuesin crime and criminal justice .

Taşkın Yıldırım, Dilvin Tan Kurtay, & Sonay Caner-Yıldırım .(2022) . Investigation of University Students' Cyber Victimization Experience in Relation to Psychological Symptoms and Social Media Use، Turkish Psychological Counseling and Guidance Journal

Yi-Kwei, Wen., Ross, B., Corotis., Carl, J., Turkstra., John, W., Reed., Jamshid, Mohammadi. (2020). Definition of Risk. 11-42. doi: 10.1201/9781003069218-2.