Hebron University Research Journal (A)
Vol. (9), pp. (129-156), 2020

H.U.R.J. is available online at
http://www.hebron.edu/journal

فاعلية برامج التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية من وجهة نظر طلبة جامعة الخليل – فلسطين

***د. مهند الجعبري، د. بلال عمرو، كلية تكنولوجيا المعلومات، جامعة الخليل**

mohanadj@hebron.edu

تاريخ التسليم: 2019 /10/22 تاريخ القبول: 2020/2/23

الملخص:

هدفت الدراسة إلى قياس فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية، والتخفيف من آثارها لدى طلبة جامعة الخليل. اعتمد الباحثان على المنهج شبه التجريبي (المجموعة الواحدة) باستخدام القياس القبلي والبعدي. اشتملت عينة الدراسة على عينة طبقية مكونة من ٧٦ طالباً وطالبة من طلبة جامعة الخليل التحقوا في مساق تطبيقات تكنولوجية في العام الأكاديمي 2019/2018. وقد خلصت الدراسة إلى وجود فروق ذات دلالة إحصائية في متوسطات التطبيقين القبلي والبعدي للجانب التقني والجانب القانوني، لصالح التطبيق البعدي وهذا يدل على فاعلية البرنامج المطبق في رفع مستوى معرفة طلبة جامعة الخليل في الجانب التقني والقانوني للحد من الجرائم الإلكترونية، فقد بلغ حجم تأثير البرنامج المطبق (٠,٦٤) بالنسبة للجانب التقني و(٠,١٤) بالنسبة للجانب القانوني. وقد اوصى الباحثان بضرورة رفع مستوى المعرفة التقني والقانوني عن طريق برامج تدريبية هادفة، وموجهة للأجيال الشابة من خلال المناهج المدرسية والجامعية، إضافة إلى تكثيف محاضرات التوعية، وورش العمل ذات العلاقة من قبل جهات الاختصاص.

الكلمات المفتاحية: التوعية، التوعية التقنية، التوعية القانونية، الجريمة الإلكترونية.

Abstract:

This research aims at investigating the effectiveness of technical and legal awareness in facing the cybercrimes and mitigation their effects among Hebron University (HU) students. The researchers depended on the quasi-experimental

methodology (one group) using pre-test and post-test. The study sample included a stratified sample of 76 students from HU who enrolled in a technology applications course in the academic year 2018/2019. The study concluded that there are statistically significant differences in the mean of the pre-test and post-test related to the technical and legal awareness among HU students, in favor for the post-test experiment. This indicates that the awareness program applied in raising the level of technical and legal knowledge among HU students to reduce cybercrime was effective with an impact of 0.62 for the applied technical awareness and 0.14 for the applied legal awareness. The researchers recommend leveraging the level of legal and technical awareness in cybercrimes by launching training programs on the level of government and the local society. They also recommend to update the school curricula to include sufficient material about the topic, and hold workshops and training sessions in the field.

Keywords: Awareness, Technical Awareness, Legal Awareness, Cybercrime.

مقدمة

تطور قطاع تكنولوجيا المعلومات والاتصالات بشكل سريع خلال العقدين الأخيرين، بحيث أصبح من الصعوبة بمكان الاستغناء عن هذه التكنولوجيا بأي شكل من الأشكال، فقد أصبحت أدوات التكنولوجيا وخدماتها جزءاً أساسياً من النشاطات اليومية للأفراد. ويرجع سبب انتشار قطاع تكنولوجيا المعلومات والاتصالات ونموها إلى عوامل عدة، أهمها: ١) تطور تكنولوجيا المعلومات والاتصالات وتوافرها. ٢) سهولة استخدام أدوات التكنولوجيا. ٣) دخول التكنولوجيا في معظم الأعمال اليومية وفي القطاعات كافة.

والمجتمع الفلسطيني كغيره من المجتمعات الأخرى تأثر بشكل كبير بهذا التطور الهائل في مجال الاتصالات وتكنولوجيا المعلومات. وتشير العديد من الدراسات والإحصائيات إلى أن هناك نمواً مستمراً ومتسارعاً في أعداد المستخدمين للتكنولوجيا والإنترنت في الأعوام الاخيرة. فحسب تقرير الجهاز المركزي للإحصاء الفلسطيني، فإن (٨٢٪) من الشباب الفلسطيني يمتلكون المهارات الأساسية اللازمة لاستخدام أدوات التكنولوجيا بما فيها استخدام خدمات الإنترنت (Palestinian Central Bureau of Statistics، 2019). ونظراً لتطور التكنولوجيا وتسهيلها للإجراءات والأعمال اليومية للمؤسسات والأفراد، فقد لجأت العديد من الشركات والمؤسسات إلى الاعتماد بشكل كبير على التكنولوجيا في تسيير أعمالها، كما لجأ معظم الأفراد إلى التكنولوجيا لتسهيل الاتصال والتواصل فيما بينهم.

رافق استخدام التكنولوجيا ووسائل الاتصال الإلكترونية ازدياد ملحوظ في معدل الجريمة الإلكترونية في فلسطين. وحسب تقارير وحدة الجرائم الإلكترونية المسؤولة عن متابعة قضايا الجرائم الإلكترونية، فإن

معدلات الجريمة الإلكترونية في فلسطين في ازدياد ملحوظ خلال السنوات الأخيرة، كما هو موضح في الجدول الآتي: (Palestinian Police Office، 2019).

جدول (1): عدد الجرائم الإلكترونية المسجلة في فلسطين

السنة	2013	2014	2015	2016	2017	2018
عدد الجرائم المسجلة	173	361	502	1327	2028	2568

وتبذل جهودٌ حثيثةٌ ومتواصلة لمكافحة الجريمة الإلكترونية في فلسطين، حيث تم إقرار قانون الجرائم الإلكترونية المعدل لعام ٢٠١٨، وتم إنشاء وحدة الجرائم الإلكترونية، كذلك تم افتتاح مركز فلسطين للاستجابة لطوارئ الحاسوب (PALCERT) في عام ٢٠١٩. وفيما يتعلق بأسباب زيادة نسبة الجرائم الإلكترونية، تشير العديد من الدراسات العالمية والمحلية إلى أن أهم تلك الاسباب يعزى إلى غياب الوعي التقني والقانوني لدى مستخدمي أدوات تكنولوجيا المعلومات، وخصوصا فئة الشباب (Amro، 2018) (Bruijn & Janssen, 2017)

مشكلة الدراسة:

إن انتشار تكنولوجيا المعلومات والاتصالات أدى إلى ظهور عديد من أشكال الجريمة الإلكترونية وانتشارها مثل انتهاك الخصوصية، الاحتيال، الابتزاز والتهديد، سرقة المعلومات وانتحال الشخصية، الخ. ويمكن تأكيد انتشار الجريمة الإلكترونية بشكل متصاعد وزيادة تأثيرها على الفرد والمجتمع في فلسطين من خلال الرجوع إلى التقارير الصادرة عن جهاز الإحصاء المركزي الفلسطيني، حيث تشير تقارير الشرطة الفلسطينية إلى أن معدل الجريمة الإلكترونية في فلسطين يتزايد بشكل كبير، كما ذكر سابقاً (Palestinian Police Office، 2019). كذلك، ثمة دراسات عديدة عالمية وعربية تبحث في أسباب ظهور الجريمة الإلكترونية وانتشارها. فمثلاً، استعرض (Al-Badainah، 2014) عدة أسباب لظهور الجريمة الإلكترونية وانتشارها منها: سهولة استهداف الضحأيا، سرعة التنفيذ وقلة التكلفة، ضعف الرقابة وصعوبة ملاحقة الجناة، الخ. ولعل أهم أسباب انتشار الجريمة الإلكترونية يعزى إلى قلة الوعي بالجوانب التقنية والقانونية لاستخدام أدوات تكنولوجيا المعلومات والاتصالات، مثل: مواقع الشبكة العنكبوتية وتطبيقات الهواتف الذكية؛ فقد ذكر تقرير مؤسسة (SANS) العالمية الخاص بأمن المعلومات الإلكترونية أن غالبية المستخدمين يفتقرون إلى المعرفة في مجال الوعي الأمني الإلكتروني، وأن المختصين يفتقرون إلى المهارات وآليات التواصل مع المستخدمين لتوعيتهم في كيفية مواجهة الجرائم الإلكترونية المختلفة والتخفيف من آثارها (SANS, 2019).

من هنا جاءت الدراسة الحالية، لكي تبين بصورة ميدانية فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية والتخفيف من آثارها، حيث تكمن مشكلة الدراسة في التساؤل الرئيس الآتي:

"ما هي فاعلية التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية طلبة جامعة الخليل؟".

ويتفرع عن هذا التساؤل الأسئلة الفرعية الآتية:

- ما هي فاعلية التوعية التقنية لدى طلبة جامعة الخليل في مواجهة الجريمة الإلكترونية؟
- ما هي فاعلية التوعية القانونية لدى طلبة جامعة الخليل في مواجهة الجريمة الإلكترونية؟

أهداف الدراسة:

تتمثل أهداف الدراسة في هدف رئيسي وأهداف فرعية. أما الهدف الرئيس فهو:

- التعرف على فاعلية التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية، والتخفيف من آثارها لدى طلبة جامعة الخليل، وينبثق عن الهدف الرئيس الأهداف الفرعية الآتية:
  - التعرف على فاعلية التوعية التقنية في مواجهة الجريمة الإلكترونية لدى طلبة جامعة الخليل.
  - التعرف على فاعلية التوعية القانونية في مواجهة الجريمة الإلكترونية لدى طلبة جامعة الخليل.
  - التعرف على وجود فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\propto \leq 0.05$) على مستوى معرفة الطلبة التقنية والقانونية، وفاعلية تلك التوعية على مواجهة الجريمة الإلكترونية في القياس القبلي والبعدي.

أهمية الدراسة:

تكمن أهمية هذه الدراسة من الناحية النظرية في ندرة الدراسات والأبحاث التي تتناول موضوع فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية في حدود علمنا، ولذلك نأمل أن تسهم هذه الدراسة في إثراء الأدب النظري بتزويد المكتبة الفلسطينية والمكتبات العربية بهذا النوع من الدراسات.

ومن الناحية التطبيقية، ستسهم هذه الدراسة في الأمور الآتية:

1. مساعدة أصحاب الاختصاص وصانعي القرار في الحكومة الفلسطينية باتخاذ الإجراءات المناسبة للحد من الجرائم الإلكترونية ومواجهتها.
2. مساعدة أصحاب القرار في مؤسسات التعليم العام والخاص باتخاذ الإجراءات اللازمة لرفع الوعي ونشر المعرفة اللازمة لمحاربة الجريمة الإلكترونية من خلال المناهج الدراسية وورش العمل والندوات والمؤتمرات.
3. رفع الوعي المجتمعي والأسري حول مخاطر الجريمة الإلكترونية والإجراءات اللازم اتخاذها لمكافحتها والحد منها.

حدود الدراسة:

- الحدود الموضوعية: هدفت هذه الدراسة إلى التعرف على مستوى وعي طلبة جامعة الخليل في الجوانب التقنية والقانونية وفاعلية ذلك في مواجهة الجريمة الإلكترونية والحد من آثارها عند استخدامهم لمواقع التواصل الاجتماعي.

- الحدود المكانية: مجال الدراسة المكاني هو جامعة الخليل في فلسطين.
- الحدود النوعية: شملت الدراسة طلبة مساق (تطبيقات تكنولوجية)، حيث إن هذا المساق متطلب جامعة اختياري ويسجل فيه طلاب وطالبات من مختلف تخصصات الجامعة ومن مختلف المستويات الأكاديمية. بعبارة أخرى شملت الدراسة عينة طبقية من طلبة جامعة الخليل.
- الحدود الزمانية: تم جمع البيانات والمعلومات الخاصة بالدراسة في عامي ٢٠١٨ و٢٠١٩.

مصطلحات الدراسة

المعرفة التقنية: وهي "الخبرة العملية والدرأية الفنية التي يمكن الاعتماد عليها في أداء المهمات" (United Nations - Economic and Social Commission for Western Asia، 1992)، كما تم تعريفها أيضا بأنها "حصيلة المعلومات الفنية للفرد والجماعة والمنظمة من خلال القدرة على اكتسابها واستيعابها والتي تسهم في حل مشكلات العمل وتحسين الأداء" (Mustafa، 1998).

المعرفة القانونية: يمكن تعريف المعرفة على أنها الفهم المكتسب بالخبرة، أو الفهم المأتي من المعلومات من خلال الدراسة والتعلم (Hornby, 1974).

كما ويعرف القانون أنه "ظاهرة تدفع بالمجتمع إلى وضع قواعد تنظم العلاقات بين الأفراد، وهذا ما يعرف "بالقانون الخاص"، وكذا سن قواعد أخرى تحكم العلاقات بين الأفراد والدولة يطلق عليها: "القانون العام"، حيث يكلَّف أشخاص من المجتمع ذاته بتنفيذ العقوبات المنصوص عليها"- (ترجمة من المصدر ((Claude, 2008).

الجريمة الإلكترونية: تعرف الجريمة الإلكترونية بأنها " كل عمل أو امتناع عن عمل يأتيه الإنسان، ويحدث أضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به"، كما تعرف أيضاً بأنها كل فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية (Al-shahri، 2009)(Bahr, 1999)

الإطار النظري

تعريف الجريمة الإلكترونية:

ثمة العديد من التعريفات المتفق عليها للجريمة الإلكترونية؛ فقد استخدم مؤتمر الأمم المتحدة العاشر لمنع الجريمة الإلكترونية المنعقد في فيينا عام ٢٠٠٠ مصطلح (جرائم الحاسب الآلي)، للدلالة على الجريمة الإلكترونية، حيث عرفها أنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية، أو داخل نظام حاسوب، حيث يشمل التعريف جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (Almoasher، 2012). وفي الاتفاقية الأوروبية الخاصة بالجريمة السيبرانية الموقعة في بودابست عام ٢٠٠١، تم استخدام مصطلح جريمة الإنترنت، وتعريفه بأنه "النشاطات غير القانونية او غير المشروعة المرتبطة بأجهزة الحواسيب واستخدام الشبكة العنكبوتية" (The Council of Euroupe، 2001).

كما وعرف طائفة من الباحثين (الجريمة الإلكترونية)، منهم الزهراني أنها "إتيان فعل غير مشروع، او الامتناع العمدي عن أداء فعل واجب الإتيان به من خلال استخدام أي وسيلة إلكترونية أو تكنولوجية بشكل غير مشروع يكون من نتيجتها الاعتداء على حقٍ من حقوق غير الشخصية أو المادية" (Al-Zahrani، 2014). وعرفها موسى أنها "النشاط الذي تستخدم فيه التقنية الإلكترونية الرقمية بصورة مباشرة او غير مباشرة باعتبارها وسيلة لتنفيذ الفعل الإجرامي المستهدف" (Musa، 2008).

من خلال التعريفات السابقة فإننا نقترح تعريف للجريمة الإلكترونية بانها " أي اعتداء متعمد على أي جهة محمية بموجب القانون يهدف إلى الحصول على منفعة مادية أو معنوية، باستخدام أي من أدوات التكنولوجيا.

ومما يذكر أن قانون الجرائم الإلكترونية الفلسطيني المعدل لعام ٢٠١٨ لم يقدم أي تعريف للجريمة الإلكترونية، وإنما تطرق إلى الكثير من المظاهر والأعمال التي تعتبر جرائم الكترونية وحدد لكل واحدة منها العقوبات المناسبة.

خصائص الجريمة الإلكترونية:

يمكن القول: إن الجريمة الإلكترونية فيها من الخصائص خلافا لما نراه في الجريمة العادية، وأهم هذه الخصائص:

- سرعة التنفيذ، وسهولة الاختفاء، والبعد عن مسرح الجريمة.
- عادة ما يستخدم الجاني مهارات مكتسبة، وبرامج خاصة، لارتكاب الجريمة الإلكترونية، إذ إن هذه البرامج تعد سريعة، ولا يشترط وجود الجاني في مسرح الجريمة لارتكاب جريمته، كما يتم استخدام تقنيات عالية الدقة تساعد الجاني في التخفي، ويصعب من اكتشافه، وقد أسهم التقدم التقني في العتاد المادي والبرمجي من سرعة تنفيذ الجريمة الإلكترونية وزيادة انتشارها (Al-Kaabi، 2009).
- تحقيقات الجريمة الإلكترونية معقدة طبقاً لطبيعة الدليل الإلكتروني:
- دليل الجريمة الإلكترونية يختلف عن دليل الجريمة العادية في أنه ليس دليلا مرئيا، ويمكن فهمه بمجرد الاطلاع على محتوياته. فدليل الجريمة الإلكترونية يتمثل في بيانات غير مرئية، صعبة الاكتشاف والمتابعة والتقصي، لأنها لا تترك أثراً واضحاً، ولا يمكن إثباتها إلا من خلال فحص فني من قبل أشخاص مؤهلين وبمهارات تقنية عالية (Abdul-Malik، 2012).

ومن المميزات الأخرى للجريمة الإلكترونية أنها تتطلب بيئة الكترونية لارتكابها، وتتم بالتعاون بين العديد من الأشخاص من أماكن مختلفة وثقافات متعددة، مما يسهل ارتكابها لسهولة توفير البيئة والأشخاص، حيث تعد الجريمة الإلكترونية عابرةً للدول بسبب سهولة حركة المعلومات عبر شبكة الإنترنت، حيث إن المجتمع الإلكتروني مجتمع منفتح لا يعرف الحدود (Al-Momani، 2010) (Herwal، 2007)، وهذا يمكن مرتكبي الجرائم الإلكترونية من ارتكاب فعلٍ إجرامٍي ضد جهة في دولة معينة من دولة أخرى (Ibrahim، 2009).

تصنيفات الجرائم الإلكترونية:

هناك اختلاف بين الباحثين في تصنيف الجرائم الإلكترونية، إذ يعود هذا الاختلاف إلى اختلاف التقنيات المستخدمة في دول العالم، واختلاف المستوى الثقافي للمجتمعات، ومدى استخدامها للتكنولوجيا الحديثة. وقد قام القحطاني (Al-Qahtani، 2014) بتصنيف الجرائم الإلكترونية ضمن ثلاث مجموعات رئيسة، هي:

1. جرائم تستهدف النظام المعلوماتي.
2. جرائم تقع باستخدام النظام المعلوماتي.
3. الجرائم التي تستغل بيئة النظام المعلوماتي.

وتحت كل مجموعة أدرج القحطاني (Al-Qahtani، 2014) قائمةً بالجرائم ذات العلاقة، فمن الجرائم التي تستهدف النظام المعلوماتي الاختراق والتلاعب في البرامج، وقرصنتها وحجب الخدمة والتجسس والتصيد. أما ما يخص الجرائم التي تقع باستخدام النظام المعلوماتي فهي سرقة المعلومات، وجرائم غسيل الأموال، وجرائم التجارة الإلكترونية، وجرائم الإرهاب عبر الإنترنت، كما أن الجرائم المخلة بالآداب العامة وانتحال الشخصية وبث الأفكار الإرهابية والمتطرفة والتخويف والتهديد فتعد من ضمن الجرائم التي تستغل بيئة النظام المعلوماتي.

آثار الجريمة الإلكترونية:

تتجلى آثار الجريمة الإلكترونية على مستويين. المستوى الأول هو مستوى الفرد، والمستوى الثاني: هو مستوى المؤسسة. فقد أصبح الفرد معتمدا اعتمادا كلياً على التكنولوجيا في إدارة شؤونه والتواصل مع الآخرين. حيث كان لهذا الاعتماد الآثار السلبية الآتية: سرقة الهوية، سرقة بطاقة الائتمان، الابتزاز والتهديد، الاحتيال ونقل ملكية الأسهم (Al-Otaibi، 2016)، إلى جانب الآثار النفسية المرتبطة بالجريمة الإلكترونية على الأفراد، منها: الانزعاج، الخوف، الانتهاك، العجز والأيذاء الجسدي (Amro، 2018).

أما فيما يتعلق بالمؤسسات الحكومية والخاصة والربحية وغير الربحية منها، فقد أصبحت تدار جزئياً او كلياً بشكل إلكتروني لسهولة تقديم الخدمات وسرعة إنجازها، ومن الجرائم الإلكترونية التي قد تتعرض لها المؤسسات والشركات سرقة الأموال، اختراق المواقع، الاطلاع على معلومات سرية والاحتيال (Bahr، 1999؛ Amro، 2018).

قانون الجرائم الإلكترونية الفلسطيني:

أصدرت دولة فلسطين بعض القوانين الخاصة التي تطرقت إلى الجرائم الإلكترونية ضمن بنودٍ بسيطةٍ هدفت إلى التخفيف من الضغوط الاجتماعية والرسمية المطالبة بملاحقة الجرائم الإلكترونية. وقد كان الإنجاز الأكبر في هذا المجال هو القرار بقانون ١٦ لسنة ٢٠١٧ بشأن الجرائم الإلكترونية، والذي قوبل بطائفة من الاحتجاجات والدعوات لتعديل العديد من البنود ذات العلاقة بحرية التعبير؛ ليتم استبداله في العام ٢٠١٨ بقانون رقم ١٠ لعام ٢٠١٨ بشأن الجرائم الإلكترونية.

قام القانون بتفصيل المخالفات الإلكترونية والعقوبات الخاصة بها، إضافة إلى تحديد الجهات ذات الاختصاص بالجريمة الإلكترونية وتوضيح صلاحياتها وواجباتها، كما حدد القانون واجبات شركات الاتصالات وتكنولوجيا المعلومات تجاه الحد من الجريمة الإلكترونية والتعاون في تحقيقاتها.

دراسات سابقة

في هذا الباب، سيتم استعراض بعض الدراسات العربية والأجنبية التي تطرقت إلى الجريمة الإلكترونية وفاعلية التوعية في مواجهة تلك الجرائم والحد من آثارها. في هذا الخصوص، أظهرت مجموعة من الدراسات والتقارير أن العديد من دول العالم وضعت إستراتيجيات، وأقرت قوانين لمواجهة الجريمة الإلكترونية، والحد من آثارها، وأحد أهم بنود هذه الإستراتيجيات يتمحور حول توعية المستخدمين التقنية والقانونية لكيفية استخدام الخدمات والمواقع الإلكترونية، وكيفية مواجهة الجرائم الإلكترونية، والحد من آثارها. فعلى سبيل المثال، عملت المملكة المتحدة على وضع إستراتيجية شاملة للأمن الالكتروني تهدف إلى تقليل مخاطر الجرائم الإلكترونية، وتزيد من موثوقية استخدام الأنظمة الإلكترونية في ممارسة الأعمال التجارية وتقديم الخدمات للأفراد والشركات عبر الإنترنت (UK Government، 2016)، كذلك أعد مكتب الأمم المتحدة المختص بالجرائم والمخدرات تقريراً مفصلاً حول الجريمة الإلكترونية، حيث خلص التقرير إلى أهمية التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية والحد من آثارها (Malby, et al., 2013). وأخيراً، اقترح الباحثان (Bruijn & Janssen, 2017) ستة قواعد إستراتيجية باعتبارها إطاراً عاماً لزيادة وعي المستخدمين في مجال الجريمة الإلكترونية وآليات مواجهتها وهي:

1. عدم تضخيم مشاكل الأمن السيبراني.
2. وضع المجتمع بصورة المجرمين وحقيقتهم.
3. تسليط الضوء على خبراء الأمن السيبراني وإنجازاتهم.
4. توضيح أهمية مكافحة الجريمة الإلكترونية للمجتمع بشكل عام.
5. ربط الأمن السيبراني بالحياة الخاصة بالأشخاص لضمان التعرف على الجرائم الإلكترونية.
6. ربط الأمن السيبراني بالبرامج السياسية لضمان إنجاح برامج مكافحة الجرائم.

بالإضافة إلى ذلك، أجرى العديد من الباحثين دراساتٍ ميدانيةً لمعرفة فاعلية توعية المستخدمين في مواجهة الجريمة الإلكترونية. فمثلاً، أجرى الحسن وآخرون (Hasan, et al., 2015)، دراسة هدفت إلى تقديم أدلة تجريبية لواضعي السياسات في مكافحة الجريمة الإلكترونية وحمأية مستخدمي الإنترنت الشباب من مخاطر الجريمة الإلكترونية وآثارها في ماليزيا. وتم إجراء التجربة الميدانية على عينة من طلاب كلية المحاسبة في جامعة مارا (University Teknologi MARA (UiTM) تتكون من (342 طالبًا وطالبة)، حيث تم توزيع استبانة تغطي المعلومات الديموغرافية وسبعاً من الجرائم الإلكترونية المعروفة. وقد أظهرت نتائج الدراسة ما يلي: (1) الطالبات أكثر وعياً ولديهن رؤى أيجابية أكثر من الذكور. (2) الطلاب في الفئة العمرية (18-23 سنة) لديهم إدراك ووعي أقل من أولئك الذين تتراوح أعمارهم بين (24

عامًا فما فوق). (3) من لديهم مؤهلات أكاديمية عليا أكثر وعياً بالجرائم الإلكترونية، ولديهم تصور مختلف لمخاطر الجرائم الإلكترونية. وأخيراً، أوصت الدراسة بضرورة تحسين سياسات مؤسسات التعليم العالي وإجراءاته في توعية الطلبة من مخاطر الجريمة الإلكترونية، مما يقلل من خطر الوقوع في شباكها وبراثنها.

كما وأجرى (Senthilkumar و Easwaramoorthy، 2017) دراسة هدفت إلى تحليل مدى الوعي بالأمن الإلكتروني لدى طلاب الجامعات في ولأية تاميل نادو - الهند، وذلك من خلال التركيز على مختلف التهديدات الأمنية والجرائم الإلكترونية. تم إجراء التجربة الميدانية من خلال توزيع استبانة على عينة من طلاب الجامعات تتكون من (٥٠٠ طالب وطالبة) من مختلف المدن في ولأية تاميل نادو. وقد أظهرت نتائج الدراسة أن حوالي (٦٩٪) من طلاب الجامعات في ولأية تاميل نادو لديهم الوعي بالأمن الإلكتروني ومخاطر الجرائم الإلكترونية المختلفة، في حين أن نسبة (٣١٪) ليس لديهم الوعي الكافي. وأخيراً، أوصت الدراسة بضرورة تحسين توعية الطلبة بالأمن الإلكتروني لتمكينهم من حمأية أنفسهم من المتسللين وتجنب مخاطر الجرائم الإلكترونية المختلفة.

وقد أجرى المعلم (Moallem، 2018) دراسة هدفت إلى معرفة مدى وعي طلاب الجامعات الذين يدرسون في أكثر البيئات تقدماً في مجال التكنولوجيا الذكية بالهجمات الإلكترونية والمخاطر الناتجة عنها وماذا يفعلون لحمأية أنفسهم. وتم البدء بإجراء الدراسة بدأية عام ٢٠١٧ على طلاب جامعتين في ولأية كاليفورنيا - وادي السيليكون وما زالت الدراسة مستمرةً. وقد أظهرت بعض نتائج الدراسة التي أجريت على عينة من الطلاب تتكون من (١٠٢ من الطلاب والطالبات) استطلعت آرائهم على النحو الآتي:

1. (٢٠٪) فقط من الطلاب يعتقدون أن لديهم معرفة ممتازة بالأمن الإلكتروني، وأن (٤٨٪) يعتقدون أن لديهم معرفة متوسطة بالأمن الإلكتروني، بينما (٣٣٪) يعتقدون أن ليس لديهم درأية بالأمن الالكتروني.
2. تشير نتائج الاستطلاع إلى أن طلاب الجامعات، على الرغم من اعتقادهم أنه يتم ملاحظتهم عند استخدام الإنترنت وأن بياناتهم غير آمنة حتى في الأنظمة الجامعية، لا يزالون غير مدركين لكيفية حمأية بياناتهم.
3. معظم الطلاب على درأية بالعواقب المحتملة لتوفير معلومات التعريف الشخصية، مثل سرقة الهوية والمطاردة، لكنهم يشعرون بالراحة عند تقديمها. ٤) المؤسسات التعليمية ليس لديها نهج نشط لتحسين الوعي بين طلاب الجامعة لزيادة معرفتهم بقضأيا الأمن الإلكتروني وكيفية حمأية أنفسهم من الهجمات الإلكترونية المحتملة، مثل سرقة الهوية أو الفدية.

أما فيما يخص فلسطين والوطن العربي، فقد أجرى كثير من الباحثين دراساتٍ ميدانيةً لمعرفة فاعلية توعية المستخدمين في مواجهة الجريمة الإلكترونية؛ منها دراسة ميدانية للتعرف على دور المؤسسة الأمنية في الحد من الجرائم المستحدثة في الضفة الغربية (Shahwan، 2018). تم إجراء الدراسة من خلال جمع المعلومات والبيانات باستخدام أدوات عديدة من عينة الدراسة التي شملت المختصين في مكافحة الجريمة الإلكترونية، وغسل الأموال في المؤسسات الامنية ومكتب النائب العام، وقد بلغ عددهم (145) مختصاً.

توصلت الدراسة إلى نتائج كثيرة من أهمها: غياب الوعي من قبل المواطنين بأنواع الجرائم الإلكترونية وطبيعتها، وكيفية التعامل معها، أو التخفيف من آثارها. وأخيراً، قدمت الدراسة توصيات عديدة أهمها ضرورة تدريب كادر أمني متخصص عملياً، وتأهيله في مكافحة الجرائم الإلكترونية، وضرورة نشر الوعي بمخاطر تلك الجرائم من خلال التعاون بين الأجهزة الأمنية والمجتمع المحلي.

كذلك، أجريت دراسة أخرى لمعرفة مدى الوعي بأمن المعلومات بين أعضاء الهيئة التدريسية والباحثين وطلاب الجامعات والموظفين في المؤسسات التعليمية في الشرق الأوسط، وتحليل العلاقة بين مستوى الوعي بأمن المعلومات والمخاطر المرتبطة به، والتأثير الكلي على المؤسسات (Al-Janabi و AlShourbaji، 2016). تم إجراء الدراسة من خلال توزيع استبانة إلكترونية، وإرسالها عبر البريد الالكتروني على عينة الدراسة التي بلغ عددها (985) مشاركاً من عدة بلدان في الشرق الأوسط، وتوصلت الدراسة إلى العديد من النتائج، أهمها أن المشاركين لا يدركون أهمية أمن المعلومات، ولا يملكون المهارات والمعارف الأساسية لتطبيق مبادئ أمن المعلومات في حياتهم اليومية. وقد أوصت الدراسة بوضع برامج التوعية والتدريب الشاملة، واعتماد جميع تدابير السلامة اللازمة على جميع مستويات المؤسسة، لضمان أن الطلاب وأعضاء هيئة التدريس والموظفين يدركون أهمية أمن المعلومات، ويملكون المهارات والمعارف الأساسية للحفاظ على بياناتهم آمنة، وبدون هذه البرامج التدريبية والتوعوية، ستكون هناك عواقب سلبية على أنظمة تكنولوجيا المعلومات، واستخدام التطبيقات الخاصة بهم، وكذلك على الأمن الشخصي للمستخدمين في الحاضر والمستقبل.

كذلك، أجريت دارسة هدفت إلى بيان أهمية وسائل التواصل الاجتماعي الإلكترونية وخصائصها، وتوعية المستخدمين من خطورة الاستخدامات السلبية لهذه الوسائل الحديثة، ومن خطورة الجرائم المستحدثة من خلالها (Bayt Al-mal، 2014). وقد أوصت الدراسة ما يلي:

1. وضع خطط توعوية مستمرة، لمواجهة الاستخدام السلبي لوسائل التواصل الاجتماعي.
2. الاستفادة من وسائل التواصل الاجتماعي، لنشر الخطط التوعوية للمستخدمين.
3. وضع أنظمة وتشريعات وقوانين تضمن التعاون فيما بين الدول للحد من الجرائم الإلكترونية، وتعمل على ضمان الاستخدام الآمن لهذه الوسائل.

وفي دراسة مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي (Gharib و Al-Amir، 2017) تم إجراء الدراسة على (٢١٤) فرد من جيل الشباب من مختلف مناطق المملكة العربية السعودية، وقد بينت الدراسة أن المعرفة بقانون العقوبات الخاص بالجرائم الإلكترونية له دور كبير في مكافحة الجرائم الإلكترونية عن طريق الحد من الممارسات السلبية عند استخدام أدوات وخدمات تكنولوجيا المعلومات.

إجراءات الدراسة ومنهجيتها

تضمن هذا الجزء عرضاً مفصلاً للطريقة والإجراءات المتبعة بهدف تحقيق أهداف الدراسة الحالية، وقد اشتمل على منهج الدراسة، ومجتمعها وعينتها، وأدواتها، والأساليب الإحصائية المستخدمة.

أولاً: منهج الدراسة:

هدفت الدراسة الحالية إلى معرفة فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية لدى طلبة جامعة الخليل. بناءً على ذلك، استخدم الباحثان المنهج شبه التجريبي القائم على المجموعة التجريبية الواحدة، وتم استخدام القياس القبلي، والقياس البعدي، حيث يعد هذا المنهج الأكثر ملاءمة لتحقيق أهداف الدراسة الحالية.

ثانياً: مجتمع الدراسة

تكون مجتمع الدراسة الحالية من جميع طلبة جامعة الخليل للعام الأكاديمي (2019-2020)، والبالغ عددهم (9500) طالبٍ وطالبةٍ.

ثالثاً: عينة الدراسة

قام الباحثان باختيار عينة قصدية من مجتمع الدراسة تكونت من (76 طالباً وطالبةً) من طلبة جامعة الخليل الذين قاموا بتسجيل مساق تطبيقات تكنولوجية[1]. يعتبر هذا المساق مساقاً اختيارياً لطلبة الجامعة من الكليات كافة ومختلف المستويات الاكاديمية (سنة أولى إلى سنة خامسة). ويمتاز أفراد العينة بأنه لم يسبق لهم أن حصلوا على برامج توعوية في مجال الجرائم الإلكترونية والتشريعات الخاصة بها. إذ تم طرح هذا الموضوع ضمن هذا الفصل لهؤلاء الطلبة. وقد جرت العادة في هذا المساق على طرح مواضيع تكنولوجية حديثة تتعلق بالحياة اليومية للمجتمع الفلسطيني، والتغيرات المجتمعية التي تأتي مع التطورات التكنولوجية بما فيها التطور السريع للإنترنت والشبكة العنكبوتية، واستخداماتها في تسيير أعمال الحكومة (الحكومة الإلكترونية)، إضافة إلى وسائل التواصل الاجتماعي والتجارة الإلكترونية. كذلك، يتضمن المساق استخدام تكنولوجيا المبلمرات الكيميائية وأثرها على قطاعات مختلفة مثل القطاع الزراعي، الصناعي، الاتصالات. وفي هذا الفصل تم التطرق إلى الجريمة الإلكترونية، أسبابها ودوافعها وطرق تجنبها. كما تم أيضا التعريف بقانون الجرائم الإلكترونية الفلسطيني وتشريعاته المختلفة الخاصة بالجريمة الإلكترونية.

---

[1] مساق تطبيقات تكنولوجية هو مساق جامعة اختياري يمكن تسجيله من جميع طلاب جامعة الخليل باختلاف مستوياتهم الأكاديمية

وصف الأداة:

قام الباحثان ببناء أداة الدراسة (الاستبانة)، حيث تم الاستعانة بالدراسات السابقة لبناء أسئلة الاستبانة، وبما يتلاءم مع الدراسة الحالية (Gharib و Al-Amir، 2017)، (Al-Janabi و AlShourbaji، 2016)، (Hasan، وآخرون، 2015). تكونت الاستبانة من محورين: المحور الأول يتعلق بالجانب التقني، ويتألف من (14) فقرة، ويهدف إلى التعرف على مدى معرفة الطلاب بالجوانب التقنية، والتي قد يتم استغلالها للقيام بأحد الجرائم الإلكترونية وفحص مدى فعالية توعية الطلبة في هذا المجال للتقليل من إمكانية التعرض لأحد أنواع الجرائم الإلكترونية. المحور الثاني يتعلق بالجانب القانوني ويتألف من (4) فقرات، ويهدف إلى التعرف على مدى معرفة الطلبة بالجوانب القانونية ومدى فعالية توعية الطلبة في هذا الجانب للتخفيف من أثار الجريمة الإلكترونية في حال حدوثها.

إجراءات الدراسة:

أولا: برنامج التوعية وجمع البيانات

أثناء تدريس مساق تطبيقات تكنولوجية، وقبل شرح القسم الخاص بالجريمة الإلكترونية، قام الباحثان بشرح أهداف الدراسة إلى طلبة المساق وتم أخذ موافقتهم على المشاركة في البحث عن طريق إجراء الاختبار القبلي والبعدي كما يلي: أولا: وفي بدأية الفصل الدراسي تم توزيع الاستبانة القبلية على جميع الطلبة على شكل نموذج جوجل (Google Form) من خلال إرسال رابط الاستبانة عبر غرفة صف جوجل (Google classroom) الخاصة بالمساق. ثانيا: تم شرح القسم الخاص بالجريمة الإلكترونية وأنواعها والجوانب التقنية والقانونية المتعلقة بها وسبل الوقأية منها ودوافع ارتكابها. كذلك، تم توعية الطلبة بمخاطر وتبعات الجرائم الإلكترونية وتم عرض إحصائيات محلية ودولية تتعلق بذلك، كما تم عرض بعض الحوادث الواقعية لبعض الجرائم الإلكترونية مع الحفاظ على خصوصية الأفراد عن طريق مختص من وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطينية. ثالثاً: تم توزيع نفس الاستبانة على الطلبة (أي الاختبار البعدي) لقياس مدى فاعلية التوعية التقنية والقانونية في مواجهة الجريمة الإلكترونية. وأخيراً، تم استخراج نتائج الاختبار القبلي والبعدي من نماذج جوجل على شكل أوراق عمل اكسل (Excel sheets) وتحضيرها للتحليل الاحصائي.

ثانياً: صدق الأداة

الصدق الظاهري: قام الباحثان بعرض المقياس في صورته الأولية على مجموعة من المحكمين من ذوي الاختصاص والخبرة في جامعة الخليل، الذين أبدوا ملاحظاتهم حول فقرات الاستبانة، وتم الالتزام بملاحظاتهم، وإخراج الأداة بصورتها النهائية.

صدق الاتساق الداخلي: تم حساب معامل الارتباط بيرسون (Pearson correlation) لفقرات كل مجال مع الدرجة الكلية للمجال، وذلك كما هو واضح في الجدول (2).

جدول (2): نتائج معامل الارتباط بيرسون (Pearson correlation) لمصفوفة ارتباط كل فقرة من فقرات المجال مع الدرجة الكلية للمجال.

الرقم	الفقرات	معامل ارتباط بيرسون (ر)	القيمة الاحتمالية (.Sig)
الجانب التقني			
.1	هل تستخدم شبكات لاسلكية مجانبة مفتوحة؟	0.52**	0.000
.2	هل تستخدم كلمات مرور مختلفة للمواقع المختلفة؟	0.78**	0.000
.3	هل تستخدم أحرفاً وارقاماً ورموزاً في كلمات المرور الخاصة بك؟	0.78**	0.000
.4	هل تستخدم كلمات مرور طويلة (أكثر من ٨خانات)؟	0.80**	0.000
.5	هل تقوم بتغيير كلمات المرور بشكل دوري؟	0.68**	0.000
.6	هل تقوم بإرسال معلوماتك الخاصة، مثل كلمة المرور عبر وسائل الاتصال مثل رسالة نصية او بريد الكتروني؟	0.69**	0.000
.7	هل تستخدم برامج مضادة للفيروسات؟	0.54**	0.000
.8	هل تقوم بتحديث البرمجيات على جهازك؟	0.77**	0.000
.9	هل تقوم بالرد على الرسائل الإلكترونية مجهولة المصدر؟	0.56**	0.000
.10	هل تقوم بتنزيل برمجيات غير موثوقة المصدر على جهازك؟	0.78**	0.000
.11	هل تستخدم وسائل حمأية للوصول لجهازك مثل كلمة المرور والبصمة والنمط وغيرها؟	0.62**	0.000
.12	هل تقوم بتجاهل الرسائل التحذيرية من جهازك عند تصفحك لمواقع معينة، او تنزيل برمجيات؟	0.61**	0.000
.13	هل يمكن استرجاع البيانات المحذوفة التي تم نشرها مسبقاً على مواقع التواصل الاجتماعي؟	0.71**	0.000
.14	تقنياً، لا يمكن الوصول إلى البيانات المخزنة على جهازك أو البيانات التي تم نشرها على مواقع التواصل الاجتماعي بشكل غير قانوني من قراصنة الإنترنت (Hackers)؟	0.73**	0.000

الجانب القانوني			
.15	يحتوي القانون الفلسطيني على قانون خاص بالجرائم الإلكترونية.	0.71**	0.000
.16	الدخول غير المصرح بها للأنظمة الإلكترونية لا يعد جريمة بل يدل على مهارة الشخص.	0.64**	0.000
.17	التجريح والإساءة للآخرين عبر مواقع التواصل الاجتماعي يعتبر جريمة إلكترونية ويعاقب عليها القانون.	0.58**	0.000
.18	نشر ملفات وبرامج خبيثة مثل الفيروسات تعد جريمة إلكترونية وليس مهارة تقنية.	0.66**	0.000

** دالة إحصائياً عند ($\alpha \leq 0.01$)، * دالة إحصائياً عند مستوى دلالة ($\alpha \geq 0.05$)

تشير المعطيات الواردة في الجدول (2) إلى أن جميع قيم مصفوفة ارتباط فقرات كل مجال مع الدرجة الكلية للمجال دالة إحصائياً، مما يشير إلى قوة الاتساق الداخلي لفقرات كل مجال من مجالات الدراسة، وهذا يعبر عن صدق المقياس المستخدم ككل.

وللتحقق من صدق الاتساق الداخلي للمجالات قام الباحثان بحساب معاملات الارتباط بين درجة كل مجال من مجالات الاداة مع الدرجة الكلية للأداة والجدول (3) يوضح ذلك.

جدول (3):نتائج معامل الارتباط بيرسون (Person correlation) لمصفوفة ارتباط درجة كل مجال من مجالات الأداة مع الدرجة الكلية للأداة.

الرقم	المجالات	معامل ارتباط بيرسون (ر)	القيمة الاحتمالية (.Sig)
.1	الجانب المادي * الدرجة الكلية	0.76**	.0000
.2	الجانب القانوني * الدرجة الكلية	0.87**	.0000

** دالة إحصائياً عند ($\alpha \leq 0.01$)، * دالة إحصائياً عند مستوى دلالة ($\alpha \geq 0.05$)

تشير المعطيات الواردة في الجدول (3) إلى أن جميع قيم مصفوفة ارتباط مجالات أداة الدراسة مع الدرجة الكلية للأداة دالة إحصائياً، مما يشير إلى قوة الاتساق الداخلي لفقرات الأداة، وأنها تشترك معا في قياس فاعلية الوعي التقني والقانوني في مواجهة الجريمة الإلكترونية والتخفيف من آثارها لدى طلبة جامعة الخليل، على ضوء المقياس الذي تم اعتماده.

ثالثاً: الثبات:

حُسب الثبات بطريقة الاتساق الداخلي وبحساب معادلة الثبات كرونباخ ألفا، وذلك كما هو موضح في الجدول (4).

جدول (4): معاملات الثبات للأداة

المقياس	عدد الفقرات	كرونباخ ألفا
		معامل الثبات
الجانب التقني	14	0.77
الجانب القانوني	4	0.84
الدرجة الكلية للمقياس	18	0.87

تشير المعطيات الواردة في الجدول (4) إلى أن قيمة معامل ثبات كرونباخ ألفا لجميع مجالات المقياس وللدرجة الكلية للمقياس كانت مرتفعة، إذ تراوحت قيم معامل ثبات كرونباخ ألفا لمجالات المقياس بين (0.77 – 0.84)، وبلغ معامل ثبات كرونباخ ألفا للدرجة الكلية للمقياس (0.87)، مما يشير إلى أن المقياس يتمتع بدرجة مرتفعة من الثبات، وهذا يشير إلى أن المقياس صالح للتطبيق، وتحقيق أهداف الدّراسة.

تصحيح المقياس:

استخدم الباحثان مقياساً مكوناً من محورين، المحور الأول المتعلق بالجانب التقني ثنائي البدائل (نعم، لا)، بحيث تعطى الإجابة (نعم) (درجتين)، وتعطى الإجابة (لا) (درجة واحدة)، والمحور الثاني المتعلق بالجانب القانوني ثلاثي البدائل، بحيث تعطى الدرجات (3، 2، 1) للبدائل (نعم، لا، لا أعلم) على الترتيب.

المدى = 2 – 1 = 1

عدد الفئات =3

طول الفئة = المدى ÷ عدد الفئات = 1 ÷ 3 = 0.33

الحد الأدنى للفئة الأولى = 1

بإضافة طول الفئة للحد الأدنى للفئة الأولى نحصل على الحد الأعلى للفئة الأولى، ونكرر هذه العملية للفئة الثانية والثالثة لنحصل على الفئات الموضحة في الجدول (5).

جدول (5): فئات المتوسطات لدرجة الجانب التقني

المتوسط الحسابي	تقييم الفاعلية
0.50-0.99	قليل
1.00-1.49	متوسط
1.50-2.00	كبير

المدى = 3 – 1 = 2

طول الفئة = المدى ÷ 3 = 2 ÷ 3 = 0.66

الحد الأدنى للفئة الأولى = 1.0

وبإضافة طول الفئة للحد الأدنى للفئة الأولى نحصل على الحد الأعلى للفئة الأولى، ونكرر هذه العملية للفئة الثانية والثالثة لنحصل على الفئات الموضحة في الجدول (6).

جدول (6): فئات المتوسطات لدرجة الجانب القانوني

المتوسط الحسابي	تقييم الفاعلية
1.00-1.66	قليل
1.67-2.33	متوسط
2.34-3.00	كبير

ثالثاً: المعالجة الإحصائية

استخدم الباحثان النسخة (26) من برنامج (Statistical Package for Social Sciences) SPSS :

نتائج الدراسة:

يشتمل هذا الجزء على النتائج التي أسفر عنها التحليل الإحصائي للبيانات، للإجابة عن أسئلة الدراسة.

نتائج سؤال الدراسة الأول: ما فاعلية التوعية التقنية لدى طلبة جامعة الخليل في مواجهة الجريمة الإلكترونية على القياس القبلي والبعدي؟

للإجابة عن السؤال الأول قام الباحثان بحساب المتوسطات الحسابية والانحرافات المعيارية في القياسين القبلي والبعدي على مقياس التوعية التقنية، والجدول (7) يوضح ذلك:

جدول (7):المتوسطات الحسابية والانحرافات المعيارية بين القياسين القبلي والبعدي على محور التوعية التقنية

الرقم	الفقرة	القياس القبلي			القياس البعدي		
		المتوسط الحسابي	الانحراف المعياري	الفاعلية	المتوسط الحسابي	الانحراف المعياري	الفاعلية
1	هل تستخدم شبكات لاسلكية مجانية مفتوحة؟	1.36	0.48	متوسط	1.66	0.48	كبير
2	هل تستخدم كلمات مرور مختلفة للمواقع المختلفة؟	1.21	0.41	متوسط	1.84	0.37	كبير
3	هل تستخدم أحرفاً وارقاماً ورموزاً في كلمات المرور الخاصة بك؟	1.07	0.25	متوسط	1.96	0.20	كبير
4	هل تستخدم كلمات مرور طويلة (أكثر من ٨خانات)؟	1.14	0.35	متوسط	1.84	0.37	كبير
5	هل تقوم بتغيير كلمات المرور بشكل دوري؟	1.37	0.49	متوسط	1.54	0.50	كبير
6	هل تقوم بإرسال معلوماتك الخاصة مثل كلمة المرور عبر وسائل الاتصال مثل رسالة نصية او بريد الكتروني؟	1.21	0.41	متوسط	1.13	0.34	متوسط

7	هل تستخدم برامج مضادة للفيروسات؟	1.55	0.50	كبير	1.67	0.47	كبير
8	هل تقوم بتحديث البرمجيات على جهازك؟	1.86	0.35	كبير	1.92	0.27	كبير
9	هل تقوم بالرد على الرسائل الإلكترونية مجهولة المصدر؟	1.05	0.22	متوسط	1.05	0.22	متوسط
10	هل تقوم بتنزيل برمجيات غير موثوقة المصدر على جهازك؟	1.25	0.44	متوسط	1.13	0.34	متوسط
11	هل تستخدم وسائل حمأية للوصول لجهازك مثل كلمة المرور والبصمة والنمط وغيرها؟	1.95	0.22	كبير	1.99	0.11	كبير
12	هل تقوم بتجاهل الرسائل التحذيرية من جهازك عند تصفحك لمواقع معينة او تنزيل برمجيات؟	1.54	0.50	كبير	1.33	0.47	متوسط
13	يمكن استرجاع البيانات المحذوفة التي تم نشرها مسبقاً على مواقع التواصل الاجتماعي؟	1.34	0.48	متوسط	1.62	0.49	كبير
14	تقنياً، لا يمكن الوصول إلى البيانات المخزنة على جهازك أو البيانات التي تم نشرها على مواقع التواصل الاجتماعي بشكل غير قانوني من قراصنة الإنترنت (Hackers)؟	1.08	0.27	متوسط	1.13	0.34	متوسط
الدرجة الكلية للتوعية التقنية		1.36	0.38	متوسط	1.56	0.36	كبير

يتضح من الجدول (7) وجود فروق ظاهرية بين المتوسطات الحسابية للقياس القبلي والقياس البعدي على محور التوعية التقنية. وللتحقق من دلالة الفروق استخدم اختبار (ت) للعينات المرتبطة (Paired-

Sample T-Test) للتعرف على الفروق بين متوسطات درجات أفراد عينة الدراسة قبل تطبيق البرنامج المستخدم وبعده، كما هو موضح في جدول (8).

جدول (8): نتائج اختبار (ت) للعينات المرتبطة (Paired- Sample T-Test) وقيمة الدلالة ومستوى الدلالة لمحور الجانب التقني للتعرف على الفروق بين متوسطات درجات أفراد عينة الدراسة قبل وبعد تطبيق البرنامج (ن=76)

المتغير	التطبيق	المتوسط الحسابي	الانحراف المعياري	قيمة (ت)	قيمة الدلالة	مستوى الدلالة
الجانب التقني	قبلي	1.36	0.12	-11.04**	0.00	دالة
	بعدي	1.56	0.11			

** دالة إحصائياً عند مستوى دلالة (0.01)، * دالة إحصائياً عند مستوى دلالة (0.05)، درجات الحرية = 75

قيمة (ت) الجدولية عند مستوى دلالة (0.05) = 1.99، قيمة (ت) الجدولية عند مستوى دلالة (0.01) = 2.64

يتضح من الجدول (8) أن قيمة (ت) المحسوبة بلغت (11.04) وهي اكبر من قيمة (ت) الجدولية عند مستوى دلالة ((0.01 التي تساوي (2.64)، وهذا يدل على وجود فروق ذات دلالة إحصائية في متوسطات التطبيقين القبلي والبعدي للجانب التقني لدى طلبة جامعة الخليل، ولصالح التطبيق البعدي. وهذا يدل على فاعلية البرنامج المطبق في رفع مستوى معرفة طلبة جامعة الخليل في الجانب التقني، للحد من الجرائم الإلكترونية.

ولمعرفة حجم فاعلية البرنامج المطبق قام الباحثان بقياس حجم التأثير من خلال معادلة مربع أيتا (η2) الآتية:

$$\eta 2 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

حيث (t): قيمة اختبار (ت)، (df): درجات الحرية

جدول (9): الجدول المرجعي المقترح لتحديد مستويات الفاعلية.

الأداة المستخدمة	الفاعلية		
	صغيرة	متوسطة	كبيرة
η2	0.01	0.06	0.14 فأكبر

والجدول (10) يوضح الفاعلية بعد تطبيق البرنامج:

جدول (10): الفاعلية للبرنامج المطبق على الجانب التقني لدى الطلبة

المحور	قيمة (ت)	مربع أيتا ((η2	الفاعلية
الجانب التقني	11.04	0.62	كبيرة

يتبين من خلال الجدول (10) أن فاعلية البرنامج المطبق كانت ذا تأثير كبير في زيادة معرفة طلبة جامعة الخليل بالجانب التقني للحد من الجرائم الإلكترونية، فقد بلغت الفاعلية بالنسبة للجانب التقني (0.62). وهذه النتيجة تجيب عن السؤال الفرعي الأول حول فاعلية الوعي التقني في مكافحة الجريمة الإلكترونية لدى طلبة جامعة الخليل، وتتفق هذه النتيجة مع ما توصل اليه (Shahwan، 2018) بان غياب الوعي المعرفي بالجريمة الإلكترونية من أسباب ارتفاع أعداد الجرائم الإلكترونية في فلسطين. كما تنسجم هذه النتائج مع ما توصل اليه (Al-Janabi و AlShourbaji، 2016) في أن أفراد الدراسة لا يملكون المهارات اللازمة، والمعارف الأساسية في امن المعلومات مما يتطلب ضرورة رفع مستوى المعرفة التقني لديهم، ومما يشير إلى ضرورة توفير التوعية التقنية للحد من الجرائم الإلكترونية والذي تم تأكيده من خلال نتائج دراستنا. كما تنسجم مخرجات هذه الدراسة جزئيا مع ما توصل إليه (Amro، 2018) بأن أحد أسباب الجريمة الإلكترونية في فلسطين هو غياب الوعي التقني والقانوني بالجريمة الإلكترونية. وحسب وجهة نظرنا فان تعزيز المعرفة بمفهوم الجريمة الإلكترونية والمهارات الأساسية في أمن المعلومات لدى الأفراد سيؤدي إلى استخدام أفضل لأدوات وخدمات التكنولوجيا الحديثة بما فيها وسائل الحمأية المختلفة التي بدورها ستؤدي إلى تقليل فرص التعرض للجريمة الإلكترونية.

نتائج سؤال الدراسة الثاني: ما هي فاعلية التوعية القانونية لدى طلبة جامعة الخليل في مواجهة الجريمة الإلكترونية على القياس القبلي والبعدي؟

للإجابة عن السؤال الثاني قام الباحثان بحساب المتوسطات الحسابية والانحرافات المعيارية في القياسين القبلي والبعدي على مقياس التوعية القانونية، والجدول (11) يوضح ذلك:

جدول (11): المتوسطات الحسابية والانحرافات المعيارية بين القياسين القبلي والبعدي على محور التوعية القانونية

الرقم	الفقرة	القياس القبلي			القياس البعدي		
		المتوسط الحسابي	الانحراف المعياري	الفاعلية	المتوسط الحسابي	الانحراف المعياري	الفاعلية
1	يحتوي القانون الفلسطيني على قانون خاص بالجرائم الإلكترونية	2.41	0.87	كبير	2.74	0.64	كبير

2	الدخول غير المصرح به للأنظمة الإلكترونية لا يعد جريمة، بل يدل على مهارة الشخص	1.83	0.57	متوسط	2.00	0.40	متوسط
3	التجريح والإساءة للآخرين عبر مواقع التواصل الاجتماعي يعد جريمة الكترونية ويعاقب عليها القانون	2.76	0.59	كبير	2.92	0.32	كبير
4	نشر ملفات وبرامج خبيثة مثل الفيروسات يعد جريمة الكترونية وليس مهارة تقنية	2.76	0.63	كبير	2.86	0.42	كبير
الدرجة الكلية للتوعية القانونية		2.44	0.66	كبير	2.63	0.44	كبير

يتضح من الجدول (11) وجود فروق ظاهرية بين المتوسطات الحسابية للقياس القبلي والقياس البعدي على محور التوعية القانونية. وللتحقق من دلالة الفروق استخدم اختبار (ت) للعينات المرتبطة (Paired-Sample T-Test) للتعرف على الفروق بين متوسطات درجات أفراد عينة الدراسة قبل تطبيق البرنامج المستخدم وبعده، كما هو موضح في جدول (12).

جدول (12): نتائج اختبار (ت) للعينات المرتبطة (Paired- Sample T-Test) وقيمة الدلالة ومستوى الدلالة لمحور الجانب القانوني للتعرف على الفروق بين متوسطات درجات أفراد عينة الدراسة قبل وبعد تطبيق البرنامج (ن = 76)

المتغير	التطبيق	المتوسط الحسابي	الانحراف المعياري	قيمة (ت)	قيمة الدلالة	مستوى الدلالة
الجانب القانوني	قبلي	2.17	0.32	3.50**	0.00	دالة
	بعدي	2.33	0.22			

** دالة إحصائياً عند مستوى دلالة (0.01)، * دالة إحصائياً عند مستوى دلالة (0.05)، درجات الحرية = 75

قيمة (ت) الجدولية عند مستوى دلالة (0.05) = 1.99، قيمة (ت) الجدولية عند مستوى دلالة (0.01) = 2.64

يتضح من الجدول (11) أن قيمة (ت) المحسوبة بلغت (3.50)، وهي أكبر من قيمة (ت) الجدولية عند مستوى دلالة ((0.01 التي تساوي (2.64)، وهذا يدل على وجود فروق ذات دلالة إحصائية في متوسطات

التطبيقين القبلي والبعدي للجانب القانوني لدى طلبة جامعة الخليل، ولصالح التطبيق البعدي. وهذا يدل على فاعلية البرنامج المطبق في رفع مستوى معرفة طلبة جامعة الخليل في الجانب القانوني للحد من الجرائم الإلكترونية.

ولمعرفة فاعلية البرنامج المطبق قام الباحثان بقياس مستوى الفاعلية من خلال معادلة مربع أيتا (η2) رقم (1)، والجدول المرجعي رقم (9).

جدول (13): يبين حجم التأثير للبرنامج المطبق على الجانب القانوني لدى الطلبة

المحور	قيمة (ت)	مربع أيتا (η2)	الفاعلية
الجانب القانوني	3.50	0.14	كبير

يتبين من خلال الجدول (13) أن مستوى فاعلية البرنامج المطبق كان ذا تأثير كبير في زيادة معرفة طلبة جامعة الخليل بالجانب القانوني للحد من الجرائم الإلكترونية، فقد بلغ مستوى الفاعلية بالنسبة للجانب القانوني (0.14).

وتجيب هذه النتيجة عن السؤال الفرعي الثاني المتعلق فاعلية المعرفة القانونية في مكافحة الجريمة الإلكترونية والحد من آثارها لدى طلبة جامعة الخليل. حيث تشير الدراسة إلى أنه للتوعية القانونية دور في الحد من الجريمة الإلكترونية. وتنسجم نتيجة هذه الدراسة مع ما توصلت اليه دراسة (Gharib و Al-Amir، 2017) والتي بينت أن المعرفة بقانون العقوبات الخاص بالجرائم الإلكترونية له دور كبير في مكافحة الجرائم الإلكترونية عن طريق الحد من الممارسات السلبية عند استخدام أدوات وخدمات تكنولوجيا المعلومات. كما يتفق (Amro، 2018؛ Hornby، 1974؛ Malby، وآخرون، 2013؛ Palestinian Police Office، 2019؛ SANS، 2019) مع دراستنا بأن عدم المعرفة القانونية بالجرائم الإلكترونية سببا في انتشار الجريمة الإلكترونية في فلسطين. ومن وجهة نظرنا، فإن المعرفة بقانون الجرائم الإلكترونية والعقوبات المترتبة عليها سيكون رادعاً للعديد من الأفراد من ارتكاب أي سلوك الكتروني مخالف للقانون كما سيكون له الأثر الكبير في توضيح السلوكيات والممارسات الخاطئة التي قد تؤول إلى ارتكاب جريمة الكترونية بقصد او بدون قصد.

التوصيات

في ضوء ما تم عرضه من نتائج الدراسة، فإن فريق البحث يوصي بما يلي:

1. ضرورة العمل على رفع الوعي التقني والقانوني اللازمين لاستخدام التكنولوجيا لدى طلبة جامعة الخليل من خلال:

a) تخصيص ورش عمل لكافة طلبة جامعة الخليل تتعلق بالتشريعات والقوانين ذات العلاقة باستخدام التكنولوجيا واستضافة مختصين في مجال التشريع والتنفيذ.

b) تخصيص مساق متخصص لطلبة الجامعة كافةً، يتم من خلاله تزويدهم بالمهارات التقنية والأدوات التكنولوجية والمعلومات ذات العلاقة بالجريمة الإلكترونية، وسبل الوقأية منها.

2. أن دور التوعية لا يتوقف على جامعة الخليل، إنما يجب أن تأخذ الحكومة دورها من خلال:

a) تفعيل دور المدرسة التوعوي من خلال إثراء المنهاج المدرسي بموضوعات توعوية وإرشادية لطرق الاستخدام الآمن لوسائل التكنولوجيا المستخدمة.

b) تفعيل تنفيذ قانون الجرائم الإلكترونية من خلال اعداد قضاة ومحامين ومحققين وتدريبهم في مجال الجرائم الإلكترونية.

c) تكثيف التعاون مع المؤسسات الوطنية ذات العلاقة بمكافحة الجريمة الإلكترونية مثل وحدة الجرائم الإلكترونية وترجمة هذا التعاون من خلال عقد محاضرات وورش عمل وزيارات تنفيذية.

d) تفعيل دور المساجد التوعوي في نشر ثقافة الاستخدام الآمن للتكنولوجيا والإنترنت.

e) تفعيل دور الاجهزة الامنية المختلفة في نشر الوعي من خلال محاضرات ومؤتمرات توعوية في هذا المجال.

3. من المهم أيضا ان يأخذ المجتمع والمؤسسات المجتمعية دورها في هذا المجال من خلال المهرجانات والمخيمات والمحاضرات وورش العمل الهادفة. ولا بد هنا من توجيه مؤسسات الحكم المحلي مثل البلديات والمجالس المحلية بدعم مثل هذه النشاطات واحتضانها لما لها من دور فعال في توعية المجتمع المحلي.

المراجع

بحر ، عبد الرحمن. (١٩٩٩). *معوقات التحقيق في جرائم الإنترنت*. (رسالة دكتوراة)، جامعة نأيف العربية للعلوم الأمنية. الرياض، المملكة العربية السعودية.

الشهري ، حسن. (٢٠٠٩). نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية. *المجلة العربية للدراسات الأمنية والتدريب* ، ٢٧ (٥٢) ، ٥١٣-٥٢٦ .

المومني ، نهلا عبد القادر. (٢٠١٠). *جرائم المعلومات*. دار الثقافة للنشر و التوزيع . عمان . الاردن.

بيت المال ، حمزة أحمد. (٢٠١٤). الإعلام ودوره في التوعية بالجرائم عبر وسائل التواصل الاجتماعي. *ملتقى: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية*. عمان . الأردن.

عبد الملك ، عماد مجدي. (2012). *جرائم الكمبيوتر و الإنترنت*. دار المطبوعات الجامعية. الإسكندرية. جمهورية مصر العربية.

شهوان ، وسيم محمد أمين أحمد. (٢٠١٨). *دور المؤسسة الأمنية في الحد من الجرائم المستحدثة في الضفة الغربية من وجهة نظر ذوي الاختصاص*. رسالة ماجستير. عمادة الدراسات العليا. جامعة القدس . القدس . فلسطين.

الكعبي ، محمد عبيد. (2009). *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت*. دار النهضة العربية. القاهرة. جمهورية مصر العربية.

ذياب موسى البدأينة. (2014). الجرائم الإلكترونية: المفهوم والأسباب. *ملتقى: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية*. عمان . الأردن.

خالد ممدوح إبراهيم. (٢٠٠٩). *الجرائم المعلوماتية*. دار الفكر الجامعي. الإسكندرية . جمهورية مصر العربية.

شعيب ابراهيم مصطفى. (1998). *أثر المعرفة التقانية والسلوك الأبداعي في مستوى أداء بعض المؤسسات الصناعية*. (رسالة دكتوراة). كلية الدراسات العليا. جامعة الموصل. الموصل. العراق.

المويشير ، تركي. (2012). *بناء نموذجي امني لمكافحة الجرائم الإلكترونية وقياس فاعليته*. ط ١. مركز البحوث والدراسات - جامعة نأيف العربية للعلوم الأمنية. الرياض . المكلكة العربية السعودية.

سعيد الزهراني. (2014). *أنظمة الجرائم المعلوماتية في دول مجلس التعاون الخليجي*، ط ١. مركز البحوث والدراسات - جامعة نأيف العربية للعلوم الأمنية. الرياض . المملكة العربية السعودية.

هروال ، نبيلة هبة. (2007). *الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات*. دار الفكر الجامعي. الإسكندرية. جمهورية مصر العربية.

موسى ، مصطفى محمد. (2008). *التحقيق الجنائي في الجرائم الإلكترونية. ط١* . دار النهضة العربية. القاهرة. جمهورية مصر العربية.

غريب ، ماجدة و الأمير ، حسن. (٢٠١٧). مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرأيم المعلوماتية السعودي. *المجلة العربية الدولية للمعلوماتية. ٥ (٧)* . ١٧-٣٢.

(١٩٩٢). *تنمية القدرات التكنولوجية الذاتية:دور المؤسسات المالية المتخصصة*. الامم المتحدة - المجلس الاقتصادي الاجتماعي. القاهرة، جمهورية مصر العربية.

العتيبي ، سليمان. (٢٠١٦). *دور البحث الجنائي في الكشف عن الجرائم المعلوماتية*. رسالة دكتوراة. قسم الدراسات الأمنية. جامعة نأيف العربية للعلوم الأمنية. الرياض. المملكة العربية السعودية.

الجهاز المركزي للاحصاء الفلسطيني. (2019). أوضاع الشباب في المجتمع الفلسطيني بمناسبة اليوم العالمي للشباب. تم الاسترجاع من الرابط:

.ItemID=3529&http://www.pcbs.gov.ps/postar.aspx?lang=ar

الشرطة الفلسطينية. (2019). الجريمة الإلكترونية جريمة العصر .. تغزو فلسطين كما المجتمعات الاخرى،

ومعظم ضحأياها من الذكورتم الاسترجاع من الرابط

http://www.palpolice.ps/ar/content/726833.html

اتفاقية بودابست. (2001). *اتفاقية بودابست لمكافحة الجرائم المعلوماتية*. بودابست: مجلس أوروبا.

القحطاني ، عبدالله. (٢٠١٤). *تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية*. رسالة ماجستير. قسم الدراسات الأمنية. جامعة نأيف العربية للعلوم الأمنية. الرياض. المملكة العربية السعودية.

References:

Abdul-Malik, I. M. (2012). *Computer and Cybercrimes.* Alexandria, The Egyptian Arabic Republic: Dar El Matboaat El Gameya.

Al-Janabi, S., & AlShourbaji, I. (2016, 02). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management, 15*(1), 30.

Al-Momani, N. A. (2010). *Information cybercrimes.* Amman, Jordan: Journal of Dar Al-shaqafa for publication and distribution .

Al-Otaibi, S. (2016). *The role of criminal investigation in the detection of information crimes.* PhD. thesis, Naif Arab University for Security Sciences, Department of Security Studies, Riyadh.

Al-Qahtani, A. (2014). *Developing criminal investigation skills in the face of information crimes.* Naif Arab University for Security Sciences, Department of Security Studies. Riyadh: Security Library.

Al-Zahrani, S. (2014). *Cybercrime Information systems in the countries of the Gulf Cooperation Council.* Naif Arab University for Security Sciences. Riyadh: Research and Studies Center.

Amro, B. (2018, 5 3). Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals. *International Journal of Wireless and Microwave Technologies(IJWMT), 8*(5), 19 - 26.

Bahr, A. (1999). *Obstacles to the investigation of cyber crime.* Naif Arab University for Security Sciences. Riyadh: The Arab Journal of Security Studies and Training.

Bayt Al-mal, H. A. (2014, ٠٩ ٠٢). Media and its role in awareness of crime through social media. *The scientific Forum on the Emerging Crimes in the Spectrum of Regional and International Changes and Transformations* (pp. 1 - 12). Amman: Forum of New crimes in light of regional and international changes and transformations.

Bruijn, H. d., & Janssen, M. (2017, 1). Building cybersecurity awareness: The need for evidence-based framing strategies. (A. Kankanhalli, G. K. Tayi, & A. Zuiderwijk, Eds.) *Government Information Quarterly , 34*(1), 1 - 7.

Claude, B. (2008). *la traduction juridique fondement et méthode.* Bruxelles: De Boeck Université.

D. M. Al-Badainah. .(2014) Cybercrimes: Soncept and Causes. *The scientific Forum on the Emerging Crimes in the Spectrum of Regional and International Changes and Transformations* .(الصفحات 3 - 28)، Amman.

Gharib, M., & Al-Amir, H. (2017, 01 31). The extent of awareness among the young age group of the Saudi information crime penal system. *International Arab Journal of Informatics., 5*(9), 17 - 32.

H Al-shahri. .(2009) Towards a unified international law to combat information crime. . *The Arab Journal of Security Studies and Training* 513 ،(52)*27* ، .526 -

Hasan, M. S., Rahman, R. A., Farah, S., Binti, H., Abdillah, T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences, 11*(4), 395 - 404.

Herwal, N. (2007). *Procedural Aspects of Cyber Crime in Evidence Collection Stage* (Vol. 1). Alexandria, The Egyptian Arabic Republic: Dar Al-feker Al-Gameey.

Hornby. (1974). *Oxford Advanced Learns, Dictionary of English.* London: Oxford University Press.

Ibrahim, K. M. (2009). *Information crimes.* Alexandria, The Egyptian Arabic Republic: Dar Al-Feker Al-Arabi.

M. O. Al-Kaabi. .(2009) *Emerging Crimes from unlawful use of the Internet.* Cairo ،The Egyptian Arabic Republic.: Dar Alnahda Al-arabia for publishing and Distribution.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). *Comprehensive Study on Cybercrime.* UNITED NATIONS, UNITED NATIONS OFFICE ON DRUGS AND CRIME. New York: UNITED NATIONS OFFICE ON DRUGS AND CRIME.

Moallem, A. (2018). Cyber Security Awareness Among College Students . *International Conference on Applied Human Factors and Ergonomics. 782*, pp. 79 - 87. Orlando, Florida: Springer .

Musa, M. M. (2008). *Criminal investigation into electronic crimes* (Vol. 1). Cairo, The Egyptian Arabic Republic: Dar Al-nahdah Al-Arabiya.

Mustafa, S. (1998). *he effect of technological knowledge and creative behavior on the performance level of some industrial establishments.* University of Mosul, College of Graduate Studies. Mosul: Journal of University of Mosul.

Palestinian Central Bureau of Statistics. .(2019 ,08 08) *The conditions of youth in Palestinian society on the occasion of the International Youth Day* .)Palestinian Central Bureau of Statistics) تاريخ الاسترداد 17 10, 2019، من Palestinian Central Bureau of Statistics: http://www.pcbs.gov.ps/postar.aspx?lang=ar&ItemID=3529.

Palestinian Police Office من ،2019 ,10 17 تاريخ الاسترداد .(2019 ,03 31) . http://www.palpolice.ps: http://www.palpolice.ps/ar/content/726833.html

SANS. (2019). *Security Awareness Report: The Rising Era of Awareness Training*. Retrieved 10 17, 2019, from https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness amongcollege students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering. 263.* IOP Publishing.

Shahwan, W. A. (2018). *The role of the security establishment in reducing the crimes committed in the West Bank from the point of view of the Specialists* . AL-Quds University, College of Graduate Studeies. Jerusalem: Al-Quds University Digital Repository service.

The Council of Euroupe. .(2001) *CONVENTION ON CYBERCRIME.* Budapest: The Council of Euroupe.

Turky Almoasher. .(2012) *Building a security model to combat cyber crime and measuring its effectiveness* .(المجلد 1) Riyadh ،Saudi Arabia: Research and Studies Center - Naif Arab University for Security Sciences.

UK Government. (2016). *NATIONAL CYBER SECURITY STRATEGY 2016 - 2021.* London: Cabinet Office and National security and intelligence.

United Nations - Economic and Social Commission for Western Asia . (1992). *SPECIALIZED FINANCIAL INSTITUTIONS AND DEVELOPMENT OF ENDOGENOUS TECHNOLOGICAL CAPABILITIES* (Vol. 1). Cairo, جمهورية مصر العربية: ESCWA United Nations FAO .