ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

أثر التوعيه بالجرائم الالكترونية خلال نظم التعلم الالكترونية لدى طلاب جامعة الملك سعود

د. اميرة القحطاني
تقنيات التعليم، كلية التربية، جامعة المجمعة، المملكة العربية السعودية
البريد الالكتروني: a.algahtani@mu.edu.sa

الملخص

هدفت هذه الدراسة لقياس درجة وعي طلاب جامعة الملك سعود بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني والإجراءات القانونية والعقوبات المتعلقة بالجرائم الإلكترونية في التعلم الإلكتروني. استخدمت الدراسة المنهج الكمي ولتحقيق أهداف الدراسة جرى تطوير استبانة ووزعت على طلاب جامعة الملك سعود المسجلين في مقررات عن بعد. و كشف تحليل البيانات أنا الطلاب لديهم وعي كبير بالجرائم الإلكترونية بسبب انتشار استخدام الإنترنت من قبل الطلاب حيث أصبح جزءاً لا يتجزأ من حياتهم اليومية.

كانت درجة وعي الطالب بالإجراءات والعقوبات القانونية المتعلقة بالجرائم الإلكترونية في التعلم الإلكتروني متوسطة. وهذا يشير إلى عدم وعي الطلاب بفاعلية الإجراءات والعقوبات الخاصة بالجرائم الإلكترونية التي يمكن تطبيقها في التعلم الإلكتروني بسبب التحول السريع في عملية التعلم في جامعة الملك سعود من التعلم التقليدي إلى التعلم الإلكتروني عن بعد الذي تم فرضه خلال فترة الدراسة في جائحة كورونا. بناءً على هذه النتائج ، قدمت الدراسة مجموعة من التوصيات التي يمكن تنفيذها لزيادة الوعي وتعظيم الاستفادة من استخدام التعلم الإلكتروني.

الكلمات المفتاحية: الجرائم، الجرائم الالكترونية، التعلم عن بعد، التعلم الالكتروني، جامعة الملك سعود.

DOI: https://doi.org/10.33193/JEAHS.33.2024.459
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

The Effect of Awareness of Electronic Crimes through E-Learning Systems among Students at King Saud University

Dr. Amirah Alghatani
College of Education, Majmah University, Kingdom of Saudi Arabia
Email:a.algahtani@mu.edu.sa

ABSTRACT

The present study endeavors to assess the level of awareness among King Saud University students regarding cybercrimes pertinent to e-learning, alongside the associated legal frameworks and penalties. Employing a quantitative methodology, the research administered a structured questionnaire to students enrolled in distance education programs at the institution. Analysis of the collected data revealed a notable degree of familiarity among students with electronic offenses, attributed to the ubiquitous integration of the Internet into their daily routines. However, students' understanding of the legal procedures and punitive measures related to cybercrimes within the context of e-learning was found to be moderately adequate. This observation underscores a potential gap in students' comprehension regarding the efficacy of established legal mechanisms and penalties for electronic offenses within the realm of e-learning. Such a gap may be ascribed, in part, to the rapid transition from conventional educational paradigms to remote e-learning modalities precipitated by the onset of the COVID-19 pandemic. Drawing from these findings, the study offers a series of recommendations aimed at enhancing awareness and optimizing the efficacy of e-learning platforms.

Keywords: crimes, cybercrimes, Distant Learning, e-learning, King Saud University.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

المقدمة :

انتشار التعليم الإلكتروني كبديل للتعليم التقليدي واجه العديد من المشاكل والتحديات بشكل عام والتحديات الأخلاقية والقانونية بشكل خاص ، نستخدم في العديد من جوانب حياتنا الشبكات الرقمية وتنغمس بشكل متزايد في بيئة الإنترنت خاصة خلال جائحة كورونا الأخير الذي يواصل العالم بأسره مكافحته. على الرغم من أن التعليم هو أحد المجالات الأكثر تضرراً من الوباء ، فإن التعلم الإلكتروني وعالمه الافتراضي يوفران بديلاً تفاعلياً اجتماعياً للمتعلمين على جميع المستويات.

ومع ذلك ، فقدأصبح التعلم الإلكتروني بيئة خصبة تمارس فيها الأعمال الخطرة. ترُتكب مجموعة متنوعة من الجرائم على منصات التعلم الإلكتروني. لقد تبنت هذه الجرائم أشكال ومشاهد جديدة وأدوات جديدة. وهكذا فإن الجرائم الإلكترونية في التعلم الإلكتروني تحظى بمساحة متزايدة في علم الإجرام .تعُرفَّ الجرائم الإلكترونية على أنها أنشطة غير قانونية لا يمكن تنفيذها إلا باستخدام جهازكمبيوتر أو شبكات كمبيوتر أو أي أشكال أخرى من تكنولوجيا اتصالات المعلومات(**Maimon, D., Louderback, E.R., 2019**) . لخص تقرير صادر عن جيمس لويس في عام 2018 إلى أن الجرائم الإلكترونية تتزايد بشكل ملحوظ حيث تبلغ الخسائر العالمية للجرائم الإلكترونية حوالي 600 مليار دولار مقارنة بـ 445 مليار دولار في عام .2014 علاوة على ذلك ، يشير التقرير إلى أن نمو الجرائم الإلكترونية على مر السنين قد تعزز من نمو سوق السوداء والعملات الرقمية (**Lewis, J.R., 2018**). يناقش بشكل مختلف أنواع الجرائم الإلكترونية ، بما في ذلك سرقة الملكية الفكرية ، وسرقة الهوية ، واختراق البريدالإلكتروني للأعمال ، وغيرها من الجرائم الإلكترونية المالية. تحتاج هذه الجرائم إلى سياسات وقوانين جديدة لتقليل مخاطرها. ومع ذلك ، تركز هذه الورقة بشكل أساسي على الجرائم الإلكترونية المرتبطة بالتعلم الإلكتروني .في التعلم الإلكتروني ، تكون المعلومات أكثر عرضة للتهديدات نظراً لأن أحداث الفضاء الإلكتروني تحدث بشكل فوري تقريباً عبر مسافات كبيرة ، ولا تتوافق حدود الشبكة مع الحدود المادية والسياسية والبيئات الرقمية عرضة للهجمات من مجموعة واسعة من المواقع (**Balkin, J,Other ,2007**). لذلك ، استغل بعض المستخدمين منصات التعلم الإلكتروني للوصول غير المصرح به إلى أنظمة المعلومات التي تستخدمها المؤسسات التعليمية والمعلمين والطلاب.

اهداف الدراسة :

تهدف هذه الدراسة إلى قياس وعي الطلاب بالاستخدام الآمن للتكنولوجيا وأدوات التعلم الإلكتروني الخاصة بها والتي تتوافق مع المعايير الأخلاقية والقانونية. تحاول الدراسة الكشف عن درجة الوعي لدى طلاب جامعة الملك سعود بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني والإجراءات القانونية والعقوبات المتعلقة بالجرائم الإلكترونية في التعلم الإلكتروني

أسئلة البحث

1) ما درجة وعي طلاب جامعة الملك سعود بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني؟
2) 2- ما درجة وعي طلاب جامعة الملك سعود بالإجراءات والعقوبات القانونية المتعلقة بالجرائم الإلكترونية في التعلم الإلكتروني؟ .
3) . ما هي المتغيرات الإحصائية (على مستوى الدلالة)) α ¼0.05) بخصوص درجة الوعي بالجرائم الإلكترونية في التعليم الإلكتروني لدى طلاب جامعة الملك سعود بناءً على متغيرات الدراسة (المقرر ، والجنس ، المرحلة الدراسية)؟
4) . ما هي المتغيرات الإحصائية (على مستوى الدلالة)) α ¼0.005) بشأن درجة الوعي بالإجراءات القانونية والعقوبات المتعلقة بالجرائم الإلكترونية في التعلم الإلكتروني لدى طلاب جامعة الملك سعود بناءً على متغيرات الدراسة (المقرر ، والجنس ، والمرحلة الدراسية) ؟

الدراسات السابقة :

منذ تأسيس التعلم الإلكتروني في الستينيات تطور بطرق عديدة. بينما لا يوجد تعريف واحد للتعليم الإلكتروني لأنه يختلف باختلاف السياق (**Campbell, L., 2004**) ، تم تعريف التعلم الإلكتروني في التعليم العالي على أنه استخدام كل من التعلم القائم على البرامج والتعلم عبر الإنترنت (**Kidd, T.T., 2009**). بالنسبة الى (**2000**

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

Weggen & Urdan،)، يغطي التعلم الإلكتروني مجموعة واسعة من التطبيقات والعمليات ، بما في ذلك التعلم القائم على الكمبيوتر ، والتعلم المستند إلى الويب ، والفصول الدراسية الافتراضية ، والتعاون الرقمي **(, (King al et ، 2009Kidd, , 2009)** حصر علماء آخرون تعريف التعلم الإلكتروني في أشكال التعلم التي تعتمد على الإنترنت أو على شبكة الإنترنت **(Keller, C., Cernerud, L., 2002) (LaRose ، .1998)** كمفهوم ، يتضمن التعلم الإلكتروني مجموعة واسعة من التطبيقات وطرق التعلم والعمليات (**Rossi, P., 2009**).

(Urdan, & Weggen, 2000) نتفق على أن التعلم الإلكتروني يمكن اعتباره اكتساب واستخدام المعرفة التي يتم توزيعها وتسهيلها بالوسائل الإلكترونية في المقام الأول.

يعد التعلم الإلكتروني كوسيلة تعليمية خالدة ولا توجد بها مسافات ، مع إمكانية الوصول إلى الطلاب في جميع أنحاء العالم.إنه يوفر للمتعلمين معرفة واسعة وفرصاً للتواصل اجتماعياً بطرق لا تستطيع البيئات التقليدية ذلك. تخلق إمكانية تبادل المعرفة والترابط بأشكال عديدة بيئة غنية ووسيلة للتعلم **(Kidd, 2009).**

أنواع التعلم الإلكتروني:

هناك طرق مختلفة لتصنيف التعلم الإلكتروني اعتماداً على مستوى المشاركة في التعليم وتوقيت التفاعل **(Algahtani, A., 2011)**.

قسم بعض العلماء التعلم الإلكتروني إلى نوعين أساسيين ، هما: التعلم الإلكتروني القائم على الكمبيوتر والإنترنت **(Algahtani, A., 2011)**. يتضمن التعلم المعتمدعلى الكمبيوتر استخدام مجموعة متنوعة من الأجهزة والبرامج المتوفرة في تكنولوجيا المعلومات والاتصالات .)ICT(علاوة على ذلك ، يمكن تقسيم وضع التعلم هذا إلى تعليم مدُار بواسطة الكمبيوتر وتعلم بمساعدة الكمبيوتر. في النوع الأول ، يتم استخدام أجهزة الكمبيوتر لتخزين واسترجاع المعلومات لدعم إدارة التعليم ، بينما يتضمن النوع الأخير استخدام أجهزة الكمبيوتر كبديل للطرق التقليدية ، بالاعتماد بشكل أساسي على البرامج التفاعلية كأداة دعم داخل الفصل أو أداة للتعلم الذاتي خارج الفصل **(Arkorful، 2015 & Abaidoo)**ومع ذلك ، فإن التعلم المستند إلى الإنترنت هو وضع أكثر تقدماً في إتاحة محتويات الدورة التدريبية على الإنترنت ، مع استعداد الروابط لمصادر المعرفة ذات الصلة ، للحصول على أمثلة لخدمات البريد الإلكتروني والمراجع التي يمكن استخدامها من قبل المتعلمين في أي وقت ومكان وكذلك توافر المعلمين أو المدربين .**(Almosa, A., 2002)**تختلف التصنيفات الأخرى لأنواع التعلم الإلكتروني اعتماداً على مدى استخدام الإنترنت أو التعلم بمساعدة الكمبيوتر. وبالتالي ، يمكن أن يتكون التعلم الإلكتروني من التعلم المدمج (أو المختلط) ، أو الوضع المساعد ، أو التعلم الإلكتروني بالكامل **(Zeitoun, H., 2008)** يدعم وضع المساعد الطرق التقليدية عند الضرورة ويوفر الوضع الممزوج درجة قصيرة المدى لطريقة تقليدية جزئياً. ومع ذلك ، فإن وضع الاتصال الكامل يتضمن الاستخدام الحصري للشبكة للتعلم **(Zeitoun, H., 2008)**. يصُنف النوع الأخير أيضاً على أنه متزامناً و غير متزامن بناءً على توقيت التفاعل **(Algahtani, A., 2011)**. يتضمن المتزامن وصولاً بديلاً عبر الإنترنت بين المعلمين أو المدرسين والمتعلمين ، أو بين المتعلمين ، وغيرالمتزامن ، ويسمح لجميع المشاركين بنشر الاتصالات إلى أي مشارك آخر عبر الإنترنت **(Algahtani, A., 2011)(Almosa, A., 2002)**. أثناء الإعدادات المتزامنة ، يمكن للطلاب إجراء مناقشات وتفاعلات مع مدرسيهم وفيما بينهم عبر الإنترنت في الوقت المحدد عبر أدوات متنوعة مثل مؤتمر الفيديو وغرف الدردشة مما يتيح لهم الاستفادة من الملاحظات الفورية في حين أن الوضع غير المتزامن أثناء السماح للطلاب بالتفاعل مع المدرسين ، لا يكون فورياً ويتم عادةً باستخدام أدوات مثل مناقشة الموضوع ورسائل البريد الإلكتروني **(Algahtani, A., 2011)(Almosa, A., 2002)**وبالتالي ، فإنه يمكنّ الطلاب من التعلم في الوقت الذي يناسبهم ،مع فقدان ميزة الاستفادة من الملاحظات الفورية من المدربين أو زملائهم الزملاء**(Almosa, A., 2002)**

التحديات الرئيسية مع التعلم الإلكتروني :

أثيرت العديد من المخاوف بشأن كفاءة التعلم الالكتروني في تزويد الطلاب بالمعرفة والمهارات السليمة. في حين تم الإشادة بالتعليم الإلكتروني باعتباره وسيلة ومنهجية تعليمية ناجحة ، لا سيما في حالة الوباء العالمي ، ظهرت

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

العديد من التحديات بشأن استخدامه على المدى الطويل. يشمل ذلك المتعلمين الذين يعانون من مشاعر الاغتراب وقلة التفاعل. وتتفاقم هذه الأمور إذا لم يكن المتعلمون يمتلكون المهارات اللازمة للمساهمة في عملية تبادل المعرفة والتفاعل الأكاديمي بين الأقران والمعلمين .على التوالي ، قد يؤثر ذلك سلباً على مهارات التنشئة الاجتماعية ويحد من دور المدربين كمديرين للعملية التعليمية (**Abaidoo & Arkorful، 2015**) قد يكون التعلم الإلكتروني كطريقة تدريس أقل إنتاجية من التفاعلات وجهاً لوجه للتوضيحات والتفسيرات. عندما يصبح الطلاب أكثر مهارة في التعلم الإلكتروني ، تصبح العديد من الظواهرغير المبررة أكثر وضوحاً. وتشمل هذه الغش والقرصنة والانتحال .بينما أثبت التعلم الإلكتروني نجاحه في العديد من التخصصات ، لا يمكن للتخصصات الأخرى الاستفادة بشكل فعال من التعلم الإلكتروني بما في ذلك المجالات العلمية التي تتطلب خبرة عملية يصعب ترجمتها عبر الإنترنت. هذا هو السبب في أن الباحثين جادلوا بأن التعلم الإلكتروني أكثر ملاءمة في العلوم الاجتماعية والإنسانية من المجالات الأخرى مثل العلوم الطبية والهندسة حيث توجد حاجة لتطوير المهارات العملية (**Abaidoo & Arkorful، 2015**)

الجرائم الإلكترونية :

تطور مصطلح الجرائم الإلكترونية مع التطور السريع للتكنولوجيا ، أصبح من الضروري حماية أنفسنا من الجرائم الإلكترونية حيث يمكن إساءة استخدام هذا التطور من قبل المهاجمين الذين يستغلون قلة وعي المستخدمين. وبالتالي ، فإنه يفرض أحد أهم المخاطر في المجالات الاقتصادية والسياسية والتعليمية والاجتماعية وغيرها في الحياة.

الجريمة الإلكترونية هي أي نشاط إجرامي تكون فيه أجهزة الكمبيوتر أو شبكات الكمبيوتر أداة أو هدفاً أو مكاناً للنشاط الإجرامي ، وتشمل كل شيء من الاختراق الإلكتروني إلى هجمات رفض الخدمة. ويشمل أيضاً الجرائم الجسدية التقليدية حيث يتم استخدام أجهزة الكمبيوترأو الشبكات لتمكين النشاط غير المشروع (**Gandhi, Thanjavur, 2012**). ومع ذلك ،قد يكون من الصعب اتخاذ قرار بشأن تعريف واحد موحد لماهية الجرائم الإلكترونية لأن بعض التعريفات ضيقة نسبياً من حيث التركيز **(Kshetri, N., 2010)** ؛ بمعنى أنها تقتصر على نوع واحد ؛ لذلك ، لا يمكن استخدامه على نطاق واسع .ساهم التطور التكنولوجي الهائل والسريع ، بوسائله التقنية ، في ظهور نوع جديد من الجريمة يعرف بالجرائم الإلكترونية. في بداية انتشار هذا النوع من الجريمة وقبل ظهورشبكات الإنترنت ووسائل الاتصال الحديثة ، استخدم بعض العلماء مصطلح الاحتيال الحاسوبي **(Kunz , Wilson, P., 2004)** للإشارة إلى هذه الجرائم لأنها كانت أكثر شيوعاً عند ظهور هذه السلوكيات. ومع ذلك ، سرعان ما أصبح المصطلح غير مناسب لطبيعة الجريمة لأن الاحتيال يعتبر نوعاً من الجرائم ، وليس مصطلحاً يمكن استخدامه ككل. بعد ذلك ، مصطلح جريمة الكمبيوتر **(Kunz , Wilson, P., 2004)** للإشارة إلى الأنشطة الإجرامية باستخدام جهاز كمبيوتر أو جهاز مشابه أو جدول بيانات أو بيانات واردة فيه .ومع ذلك ، فإن هذا المصطلح ليس دقيقاً لأنه يركز فقط على عنصر أساسي مستخدم في الجريمة (أي الكمبيوتر) ، وبالتالي يتجاهل الأدوات الأخرى المستخدمة في مثل هذه الجرائم.

علاوة على ذلك ، فإن المصطلح العام يشمل الجرائم المرتكبة ضد المكونات المادية لجهاز الكمبيوتر من جهة ، والآخر يستثني الجرائم المرتكبة حيث يكون الكمبيوتر مجردأداة لتنفيذ عمل إجرامي مثل الاحتيال .مصطلح آخر ، إساءة استخدام الكمبيوتر **(Kerr, O.S., 2003)** ، يبدو أنه يتضمن مشكلات أكثرأهمية تتعلق بالكمبيوتر ، لكن المصطلح غير دقيق لأن بعض الممارسات الخاطئة التي تستند إلى الكمبيوتر قد لا ترقى إلى مستوى جريمة جنائية ، وقد تم ارتكاب العديد من الجرائم من خلال الاستخدام المشروع للكمبيوتر. بعد ذلك ، ظهر مصطلح جريمة تكنولوجيا المعلومات والاتصالات كمحاولة لتغطية جميع الجرائم ذات الصلة ، لكنه لم يكن شاملاً أيضاً لأنه يستبعد الجرائم التي لا يكون فيها الجهاز متصلاً بشبكة معينة .ظهرت العديد من المصطلحات والعبارات لتحديد وتعريف هذه الجرائم ؛ ومع ذلك ، فإن التطور التكنولوجي السريع وثورة المعلومات التي خلقت أجهزة الكمبيوتر والأجهزة الداعمة والأدوات ، تليها أنظمة المعلومات والإنترنت والتطبيقات والبرامج ، جعلت من الصعب مواكبة هذه التطورات والممارسات الإجرامية. في النهاية ، ظهر مصطلح الجرائم الإلكترونية ، لكن تعريفاً محدداً يخضع للجدل.

وبالتالي ، لم يتم التوصل إلى توافقفي الآراء بشأن تعريف هذه الجرائم. وبالتالي ،يمكن تعريف الجرائم الإلكترونية بطريقتين. يركز التعريف الأول على وسائل ارتكاب الجريمة ، في حين أن أي جريمة ترتكب

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

باستخدام أي جهاز إلكتروني أو رقمي أو باستخدام أي وسيلة اتصال على شبكة الكمبيوتر أو تقنية المعلومات هي جريمة إلكترونية.على سبيل المثال ، الاحتيال عبر الإنترنت هو جريمة إلكترونية يستخدم فيها المجرم الكمبيوتر أو الهاتف الذكي للوصول إلى الإنترنت والتواصل مع الضحية لتنفيذ الفعل الإجرامي. يركز التعريف الثاني على موضوع الجريمة ومكانها. على سبيل المثال ، إذا تم ارتكاب انتهاكات إلكترونية على البيانات أو أنظمة المعلومات أو مواقع الويب أو الشبكات الداخلية أو محتويات أجهزة الكمبيوتر أو أقراص التخزين أو أي جهاز رقمي أو غير رقمي يحتوي على بيانات أو معلومات ، فإنه يعتبر أيضاً جريمة إلكترونية .ومن ثم ، من الصعب حصر تعريف الجريمة الإلكترونية في تعريف محدد وشامل بالنظرإلى التطبيق الواسع لهذه الجرائم وتطور تكنولوجيا المعلومات ، التي تخلق باستمراروسائل إلكترونية وتكنولوجية جديدة.

خصائص الجرائم الإلكترونية :

تشيرالأبحاث السابقة إلى أن للجرائم الإلكترونية طبيعة فريدة تميزها عن الجرائم التقليدية لأنها مرتبطة بأنظمة المعلومات وأجهزة الكمبيوتر والبيانات ومن المرجح أن يرتكبها مجرم أكثر دراية من المجرمين التقليديين حيث يستخدم مجرمو الإنترنت التكنولوجيا الحديثة أو يستهدفونها. (**Kshetri, N., 2010b**). وبالتالي ، فإن خصائص الجرائم الإلكترونية تشمل. :

1- يعتبر العنصر التكنولوجي من أهم سمات الجرائم السيبرانية. وبالتالي ، يمكن أن تكونالتكنولوجيا وسيلة أو مكان ارتكاب الجريمة. لذلك فهي ذات طبيعة فنية

2. .ليس من السهل اكتشاف الجرائم الإلكترونية وإثباتها. تتميز هذه الجريمة بعدم وجود قضايا مكتسبة مقارنة بالجرائم التقليدية بسبب طبيعتها الفنية ، والتي قد تنطوي فيكثير من الأحيان على بعض التعقيد أو إحجام بعض الشركات ومقدمي الخدمات عن الإبلاغ عن مثل هذه الجرائم للحفاظ على سرية العملاء. علاوة على ذلك ، ليس للجرائم الإلكترونية تأثير مادي ملموس لأنها تركز على أنظمة المعلومات حيث يمكن محوالأدلة وحذفها بسهولة. علاوة على ذلك ، يختلف وعي الناس أيضاً بين طبقاتمختلفة من المجتمع ، حيث قد يتعرض العديد من الأشخاص لهجمات على أنظمةالبيانات والمعلومات الخاصة بهم دون أن يعرفوا حقاً أنهم تعرضوا للهجوم .وبالتالي ،يمكن إخفاء الأدلة غير المادية على هذه الجرائم والتخلص منها بسهولة بسببعدم وجود تأثير خارجي لهذه الجرائم حيث يتم تنفيذها من خلال نبضات كهربائيةحيث يمكن تغيير الأرقام والبيانات ومحوها بسهولة. بالإضافة إلى ذلك ، فإن الجاني في هذه الجريمة عادة ما يكون غير موجود في مسرح الجريمة ولكنه يرتكب الجريمة عن بعد باستخدام الإنترنت ، ولا يترك أي دليل مادي على وجوده .علاوةعلى ذلك ، هناك العديد من الأجهزة والخوادم التي تحتوي على ذاكرة مليئة بالبيانات أو متصلة بشبكة معلومات تحتوي على كمية هائلة من البيانات والمعلومات التي لا يمكن للأفراد مراجعتها والتحقق منها. لذلك ، قد تُفقد بعض الأدلة القاطعة في هذهالأجهزة ، مما يجعل الاحتفاظ بها ومراجعتها أمراً صعبا

3. ً. الطابع الدولي لهذه الجرائم يختلف عن التقليدية. ارتبطت الجرائم الإلكترونية ارتباطاً وثيقاً بأنظمة المعلومات والإنترنت ووسائل الاتصال الحديثة الأخرى. وبالتالي ، في الطبيعة ،ليس لديهم حاجز جغرافي أو حد سياسي يحجبها عن دولة معينة. لذلك ، فإن تأثير الجرائم الإلكترونية يمتد إلى العالم بأسره لأن هذه الخاصية تمكن المجرمين من ارتكاب جريمة في بلد ما ومراقبة نتائجها في دولة أخرى في جميع أنحاءالعالم. ومن ثم ، قد يصل الضرر إلى الضحية أينما وجدت.

الجرائم الإلكترونية والتعلم الإلكتروني :

في الوقت الحاضر ، مع الوضع الحالي في العالم ، تحولت المؤسسات التعليمية من التعلم في الحرم الجامعي إلى التعلم الإلكتروني. ومن ثم ، فقد زادت احتمالية وقوع هجمات إلكترونية. ومع ذلك ، تم توجيه القليل من الاهتمام في البحث إلى مسألة الوعي بأمن التعلم الإلكتروني ، خاصة وأن معظم الأبحاث تناقش الوعي بالأمن السيبراني بشكل عام(**Raheem, B.R., Khan, M.A., 2020**) (**Venter ,2019**على أهمية الوعي بالأمن السيبراني في المدارس والأساليب التي يستخدمها أصحاب المصلحة لتعزيز الأمن السيبراني بالإضافة إلى العديد من التحديات ، مثل نقص الخبرة والتمويل والموارد(**Bele, , M., Rozman, D., Jemec, 2014**)كما أكد على أهمية توعية الطلاب للوقاية من الجرائم الإلكترونية بشكل عام. وخلصوا إلى أنه من الأهمية بمكان خلق

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

جهد مشترك لأصحاب المصلحة الرئيسيين لزيادة الوعي. وبالتالي ، فقد أعدوا دورات تعليمية مختلطة لتعزيز الوعي بهذه القضية (**Chandarman, R., Van Niekerk, B., 2017**).

ناقش نفس الموضوع على طلاب المرحلة الجامعية. في المقابل ، قاموا باختبار وعي الطلاب في مؤسسات التعليم العالي الخاصة حول الجرائم الإلكترونية باستخدام استبيان يختبر معرفتهم بمصطلحات مختلفة تتعلق بالأمن السيبراني. وخلصوا إلى أن هناك حاجة أساسية لتعزيز الوعي بالأمن السيبرانيبين جمهورهم(. **Poonia, , Bhardwaj, A., 2012**)ناقش أيضاً الدور الحيوي لوجود أخلاقيات الإنترنت في بيئات التعلم الإلكتروني ، وفهم مخاطر السلوك الضار وغير القانوني ، وتعلم كيفية حماية أنفسنا ومستخدمي الإنترنت الآخرين من مثل هذا السلوك. كما يتضمن تعليم الشباب الذين قد لا يدركون احتمال إلحاق الأذى بأنفسهم والآخرين عبر الإنترنت .

ركزت الدراسات السابقة على وعي الطلاب بالجرائم الإلكترونية بشكل عام ولم تستكشف العلاقة بين الجرائم الإلكترونية وتأثيرها على التعلم الإلكتروني.

وأكدت على ذلك دراسة (عيده سليمان ، عبدالله المهداوي ، 2023) والتى هدفت إلى معرفة مستوى الوعي بنظام مكافحة الجرائم المعلوماتية لدى طلبة الدراسات العليا بـجامعة تبوك، والكشف عن وجود فروق في مستوى الوعي وفقًا لمتغير: (الجنس، والمستوى الدراسي، والكلية، والدورات التدريبية في مجال الجرائم المعلوماتية والأمن السيبراني) ولتحقيق أهداف البحث تم استخدام المنهج الوصفي الاستقرائي، وتم تصميم استبانة تكونت من (34) فقرة موزعة على محورين، طُبقت على عينة عشوائية طبقية بلغت (139) فردًا من طلبة الدراسات العليا بجامعة تبوك.

وتوصلت الدراسة إلى نتائج عدة أهمها: أن مستوى الوعي بالجرائم الواردة بنظام مكافحة الجرائم المعلوماتية لدى عينة الدراسة كان (متوسطًا)، وقد بلغ متوسطه (1.84)، وجاء مستوى الوعي بالعقوبات الواردة بنظام مكافحة الجرائم المعلوماتية (مرتفعًا)، وقد بلغ متوسطه (2.52). وفي ضوء النتائج قُدِّمت توصيات أهمها: نشر الوعي بنظام مكافحة الجرائم المعلوماتية؛ ليتم استخدام الشبكة المعلوماتية والأجهزة الإلكترونية بالشكل الملائم الذي يساعد على تجنب المخاطر التي تنتج عن سوء استخدامها.

ودراسة (سها رجب ،2023) والتى تهدف إلى التعرف على مدى وعي الشباب بالعوامل التي تؤدي إلى تزايد الجرائم وانتهاك خصوصية الفرد، والكشف عن مدى وعي الشباب من مستخدمي الإنترنت بأساليب الجرائم الإلكترونية في انتهاك خصوصية الفرد، وتحديد مدى وعيهم بالآثار الاجتماعية المترتبة على انتهاك خصوصية الفرد عند التعرض للجرائم الإلكترونية، والتوصل لمقترحات تخفف من الآثار الاجتماعية المترتبة على انتهاك خصوصية الفرد من الجرائم الإلكترونية من وجهة نظر الشباب، كذلك الكشف عن طبيعة العلاقة بين الأساليب المتبعة في الجرائم الإلكترونية والآثار الاجتماعية المترتبة عليها، وتحديد الفروق في الآثار الاجتماعية للجرائم الإلكترونية باختلاف الخصائص الاجتماعية بعينة الدراسة، وقد اتخذت الدراسة نظرية التفاعلية الرمزية ونظرية المخالطة الفاصلة منطلقا نظريا لها، وقد اعتمدت على استبيان يقيس وعى الشباب الجامعي نحو خطورة الجرائم الإلكترونية في انتهاك خصوصية الفرد، وتمثل المجال البشري للدراسة الحالية بعينة عشوائية بسيطة من طلاب الفرقة الرابعة المعهد العالي للخدمة الاجتماعية بالقاهرة بنسبة (10%) من الطلاب فبلغت عينة الدراسة (160) مفردة، وكانت أهم النتائج التي توصلت لها الدراسة أنه توجد علاقة طردية جوهرية دالة عند مستوى معنوية (α 0.05) بين الأساليب المتبعة في الجرائم الإلكترونية والآثار الاجتماعية المترتبة عليها من وجهة نظر الشباب.

الجرائم الإلكترونية وتسريب الوثائق والمعلومات السرية بجامعة الملك سعود

وفقا لنظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية (الإدارة العامة للأمن السيبراني بجامعة الملك خالد ، 2023) يجب مراعاة التالي:

1) دخولك بطريقة متعمدة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لك بالدخول إليها يعتبر مخالفا للقوانين ويعرضك للعقوبة بالسجن مدة لا تزيد على عشرة سنوات وبغرامة لا تزيد عن خمسة ملايين ريال، أو بإحدى هاتين العقوبتين.
2) تنصتك على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه يعتبر مخالفة قانونية وفقا لنظام مكافحة الجرائم المعلوماتية ويعرضك للعقوبة

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين وفقا لنظام مكافحة الجرائم المعلوماتية.

3) وصولك (دون مسوغ نظامي صحيح) إلى بيانات شخصية أو بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تُتيحه من خدمات يعد جريمة و يعرضك للعقوبة بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال، أو بإحدى هاتين العقوبتين.

4) قيامك بإيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير أو مسح البرامج، أو البيانات الموجودة أو المستخدمة فيها أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها يعد مخالفا ويعرضك للعقوبة بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين وفقا لنظام مكافحة الجرائم المعلوماتية.

5) دخولك الغير مشروع إلى موقع إلكتروني أو خدمة تخص جامعة الملك خالد، لتغيير تصميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه أو إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها بأي وسيلة كانت تعد جريمة إلكترونية و يعرضك للعقوبة بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين وفقا لنظام مكافحة الجرائم المعلوماتية.

6) تشهيرك بالآخرين ، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة يعد جريمة و يعرضك للعقوبة بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين وفقا لنظام مكافحة الجرائم المعلوماتية.

7) دخولك المشروع أو الغير مشروع على أنظمة جامعة الملك خالد لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا يعد جريمة و يعرضك للعقوبة بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.

8) مساسك بالحياة الخاصة عن طريق إساءة استخدام البيانات الناتجة عن دخولك المشروع أو غير المشروع لأنظمة الجامعة ، أو ما في حكمها يعد جريمة ويعرضك للعقوبة بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.

9) دخولك غير المشروع إلى انظمة أو مواقع جامعة الملك خالد مباشرة ، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني يعد جريمة ويعرضك للعقوبة بالسجن مدة لا تزيد على عشرة سنوات وبغرامة لا تزيد عن خمسة ملايين ريال، أو بإحدى هاتين العقوبتين.

إجراءات الدراسة وأدواتها

اتبعت الدراسة أداة الاستبانة لجمع المعلومات والبيانات اللازمة، لمناسبتها للمنهج المتبع في الدراسة، والأكثر ملائمة لتحقيق أهدا فها والإجابة على تساؤلاتها .وقد تم الاعتماد عند إعداد الاستبانة بالاطلاع على الأدبيات والدراسات السابقة المتعلقة بموضوع الدراسة،والأخذ بأراء المحكمين الذين عرضت عليهم الاستبانة في صورتها المبدئية بما يتناسب مع أهداف الدراسة؛ وبناء على ذلك تم تصميم

أداة الاستبانة وقد تكونت من قسمين وهما كالآتي:

أ -**القسم الأول** :يشتمل الجزء الأول على البيانات الأولية لأفراد عينة الدراسة كما على النحو الآتي:
(النوع، المرحلة الدراسية، المقرر الدراسي.)

ب -**القسم الثاني** :يشتمل الجزء الثاني على محاور الاستبانة وهي كما على النحو الآتي:

– **المحور الأول** :الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني بجامعة الملك سعود ، واحتوى على (3) عبارات

– **المحور الثاني** :من وجهة نظرك ماهي ما مدي الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني بجامعة الملك سعود ؟، واحتوى على (27) عبارة

– **المحور الثالث** :من وجهة نظرك ماهي أبرزالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ؟، واحتوى على (8) عبارات .

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

وقد تم توزيع الاستبانة على مجتمع الدراسة البالغ عددهم (1829) طالباً وطالبة، وتم أخذ عينة عشوائية ممثلة لمجتمع الدراسة بلغ عددها (317) طالباً وطالبة، وذلك وفق ما حدده جدول كرجسي ومورغان (Krejcie & Morgan, 1970)، وبذلك يكون عدد الاستبانات التي تم تحليلها (317) استبانة صالحة للتحليل الإحصائي.

صدق أداة الدراسة:

أ- صدق الاتساق الظاهري لأداة الدراسة:

للتحقق من الصدق الظاهري للاستبانة تم عرضها على مجموعة من المحكمين المتخصصين من أعضاء هيئة التدريس في قسم علم المعلومات بجامعة الملك سعود ، وفي ضوء أرائهم ومقترحاتهم تم تصميم أداة الدراسة .

ب -صدق الاتساق الداخلي لأداة الدراسة:

بعد التأكد من الصدق الظاهري لأداة الدراسة تم حساب معامل الارتباط بيرسون لمعرفة الصدق الداخلي للاستبانة، وذلك عن طريق حساب معامل الارتباط بين درجة كل عبارة من عبارات الاستبانة بالدرجة الكلية للمحور الذي تنتمي إلية العبارة، كما هو موضح في الجداول الآتية(4) 3 (3) (2) (1)

جدول رقم (1) معاملات ارتباط بيرسون لعبارات المحور الثاني(من وجهة نظرك ماهي أسباب ضعف الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني بجامعة الملك سعود ؟)

رقم العبارة	معامل الارتباط
1	**0.553
2	**0.716
3	**0.686

جدول رقم (2) معاملات ارتباط بيرسون لعبارات المحور الأول (الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني بجامعة الملك سعود)

رقم العبارة	معامل الارتباط
1	**0.554
2	**0.645
3	**0.514
4	**0.539
5	**0.526
6	**0.478
7	**0.417
8	**0.432
9	**0.623
10	**0.628

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

**0.537	11
**0.537	12
**0.459	13
**0.437	14
**0.553	15
**0.716	16
**0.686	17
**0.752	18
**0.735	19
**0.495	20
**0.559	21
**0.843	22
**0.838	23
**0.794	24
**0.612	25
**0.521	26
**0.710	27

**دال عند مستوى الدلالة 0.01 فأقل

جدول رقم (3) معاملات ارتباط بيرسون لعبارات المحور الثالث(من وجهة نظرك ماهي مدى الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ؟

رقم العبارة	معامل الارتباط
1	**0.510
2	**0.682
3	**0.704
4	**0.661
5	**0.591
6	**0.721
7	**0.687

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

8	**0.671

يتضح من الجداول السابقة رقم (1 – 2 – 3) ما يأتي:
أن قيم معامل ارتباط كل عبارة من العبارات مع المحور الذي تنتمي له موجبة ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل، ممايدل على صدق الاتساق الداخلي بين عبارات المحور والدرجة الكلية للمحور، وتمتعها بدرجة صدق عالية صلاحيتها للتطبيق.

ثبات أداة الدراسة:

لقياس مدى ثبات أداة الدراسة (الاستبانة)تم استخدام(معادلة ألفا كرونباخ) Cronbach's Alpha (α) للتأكد من ثبات أداة الدراسة ، والجدول رقم (4) يوضح معاملات ثبات أداة الدراسة .

جدول رقم (4) معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

محاور ابعاد الاستبانه	عدد العبارات	معامل ألفا كرونباخ
المحور الأول: ما مدى الوعى بماهية الجرائم الالكترونية ؟	3	0.78
المحور الثاني: ما مدي الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني ؟	27	0.73
المحور الثالث مامدي الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ؟	8	0.80
معامل ثبات الاستبانه	38	0.70

يتضح من الجدول رقم (4) ما يأتي:

أن معاملات ثبات ألفا كرونباخ كانت مرتفعة في جميع المحاور، وأن معامل الثبات العام قد بلغ (0.70)، وهذا يدل على أن الاستبانة تتمتع بدرجة عالية من الثبات يمكن الاعتماد عليها في التطبيق الميداني للدراسة.

أساليب المعالجة الإحصائية:

لتحقيق أهداف الدراسة وتحليل بياناتها اتبعت الدراسة عدداً من الأساليب الإحصائية المناسبة باستخدام الحزم الإحصائية للعلوم الاجتماعية، والتي يرمز لها اختصارا بالرمز (SPSS) وذلك بعد أن تم ترميز البيانات وإدخالها إلى الحاسب الآلي، ثم استخرجت النتائج وفقاً للأساليب الإحصائية الآتية:

1) التكررات والنسب المئوية؛ لوصف خصائص أفراد عينة الدراسة .
2) المتوسطات الحسابية والانحراف المعياري :لمعرفة اتجاهات إجابات أفرادعينة الدراسة لكل عبارة من عبارات الاستبانة، إلى جانب المحاور الرئيسية
3) معامل ارتباط بيرسون(Pearson) لقياس صدق الاتساق الداخلي بين عبارات كل محور تنتمي إليه عبارات هذا المحور.
4) معامل الثبات ألفا كرونباخ (Cronbach's Alpha(α) Cronbach's Alpha(α)) لحساب معامل ثبات أداة الدراسة .

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

معيار الحكم على نتائج الدراسة:

لتسهيل تفسير النتائج تم اتباع الأسلوب الآتي لتحديد مستوى الإجابة على بدائل المقياس، وذلك بإعطاء وزن للبدائل(:مدرك =3، مدرك إلى حد ما 2 = ، غير مدرك)1 = ، كما يتضح من الجدول رقم)6 (، ثم صنفت تلك الإجابات إلى ثلاثة مستويات متساوية المدى عن طريق المعادلة الآتية:

عدد بدائل المقياس (÷ (= طول الفئة(= أكبر قيمة-أقل قيمة(0.66 =) 3 (÷ 1 - 3)

جدول رقم (5) درجات فئات معيار نتائج الدراسة وحدودها وفقًا لمقياس ليكرت الثلاثي

الدرجة	معيار الحكم على النتائج	فئة المتوسط	
		من	إلى
5	موافق	2.34	3.00
2	محايد	1.67	2.33
1	غير موافق	1.00	1.67

(
أقل أثرا 5 = ، أثر ضعيف 4 = ، أثر متوسط 3 = ، مؤثر2 = ، أكثر أثرا) 1 =، كما يتضح من الجدول رقم ( )7، ثم صنفت تلك الإجابات إلى خمس مستويات متساوية المدى عن طريق المعادلة الآتية:

عدد بدائل المقياس (÷ (= طول الفئة(= أكبر قيمة-أقل قيمة(0.80 =) 4 (÷ 1 - 4 وللحصول على مدى المتوسطات التالية لكل وصف أو بديل.

عرض نتائج الدراسة ومناقشتها

أولاً :وصف خصائص عينة الدراسة:

جدول رقم (6) توزيع أفراد عينة الدراسة وفقاً لمتغير النوع

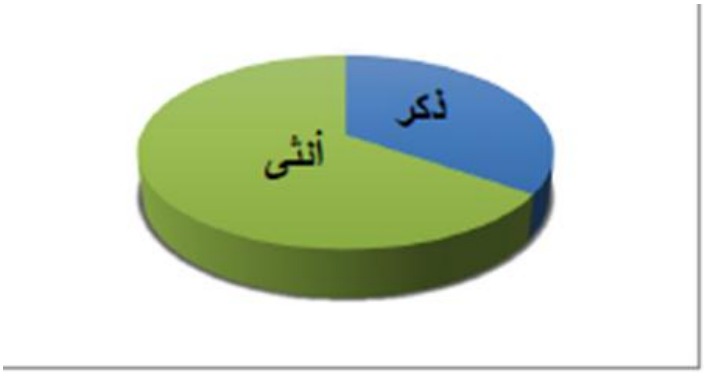
النوع	التكرار	النسبة
ذكر	109	%34.7
أنثي	207	%65.3
المجموع	317	100٪

يتضح من الجدول رقم (7) ما يأتي:

أن (207) من أفراد عينة الدراسة يمثلون ما نسبته 65.3 ٪ من إجمالي أفراد عينة الدراسة إناث وهن الفئة الأكثر من أفراد عينة الدراسة ، كما أن (109) منهم يمثلون ما نسبته 34.7 ٪ من إجمالي أفراد عينة الدراسة ذكور.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

شكل بياني رقم (1) توزيع أفراد عينة الدراسة وفقاً لمتغير النوع

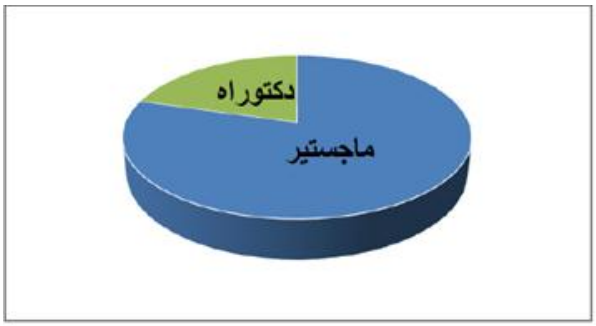


جدول رقم (7) توزيع أفراد عينة الدراسة وفقاً لمتغير المرحلة الدراسة

المرحلة الدراسية	التكرار	النسبة
ماجيستير	227	%79.5
دكتوراة	90	%20.5
المجموع	317	100٪

حيث أن (227) من أفراد عينة الدراسة يمثلون ما نسبته 79.5 ٪ من إجمالي أفراد عينة الدراسة بمرحلة الماجستير وهم الفئة الأكثر من أفراد عينة الدراسة ، كما أن (90) منهم يمثلون ما نسبته 20.5 ٪ من إجمالي أفراد عينة الدراسة بمرحلة الدكتوراة

شكل بياني رقم (2) توزيع أفراد عينة الدراسة وفقاً لمتغير المرحلة الدراسي



جدول رقم (8) توزيع أفراد عينة الدراسة وفقاً لمتغير المقرر الدراسي

المقرر الدراسي	العدد	النسبة
الاخلاق و القيم الانسانية	90	%33.7
مهارات التواصل	125	%34.4

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

الثقافة الوطنية	75	%31.9
المجموع	317	100٪

أن (125) من أفرادعينة الدراسة يمثلون ما نسبته34.4% من إجمالي أفراد عينة الدراسة يدرسون بمقرر (مهارات التواصل) وهم الفئة الأكثرمن أفراد عينة الدراسة ، بينما أن (90) من أفرادعينة الدراسة يمثلون ما نسبته33.7% من إجمالي أفراد عينة الدراسة يدرسون بمقرر (الاخلاق و القيم الانسانية) ، في حين أن (75) من أفرادعينة الدراسة يمثلون ما نسبته31.9%من إجمالي أفراد عينة الدراسة يدرسون بمقرر (الثقافة الوطنية)

ثانياً :النتائج المتعلقة بتساؤلات الدراسة

التساؤل الأول :ما مدى الوعى بماهية الجرائم الالكترونية المتعلقة بالتعلم الإلكتروني لدى طلاب بجامعة الملك سعود ؟

للتعرف على مدى الوعي بماهية الجرائم الالكترونية لدى طلاب وطالبات الدراسات العليا بجامعة الملك سعود تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الأول :الوعي بماهية الجرائم الالكترونية لدى طلاب وطالبات الدراسات العليا بجامعة الملك سعود ، وجاءت النتائج كما يوضحها الجدول الآتي:

جدول رقم (9) إجابات أفراد عينة الدراسة على المحور الثانى: الوعي بماهية الجرائم الالكترونية لدى طلاب بجامعة الملك سعود

	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعيارى	الترتيب
		النسبة	موافق	محايد	غير موافق			
1	هل تعلم ما المقصود بالجريمة الإلكترونية	ك	219	47	51	2.91	0.757	13
		%	69.1	14.8	16.1			
2	هل هناك فرق بين الجريمة الإلكترونية والجريمة التقليدية	ك	204	43	70	2.42	0.829	14
		%	64.4	13.6	22.1			
3	هل سبق لك أن وقعت ضحية لجرائم إلكترونية	ك	291	24	2	2.53	0.306	2
		%	91.8	7.6	0.6			

أن هناك تجانس في موافقة أفراد عينة الدراسة على مدى الوعي بالجرائم الإلكترونية ،حيث تراوحت متوسطات موافقتهم على مدى الوعي بالجرائم الإلكترونية ما بين (2.53إلى 2.91)، وهي متوسطات تقع في الفئة الثالثة من فئات المقياس الثلاثي والتي تشير إلى" موافق "في أداة الدراسة .

وهذا مؤشر إيجابي مما يدل على أن أفرادعينة الدراسة لديهم ثقافة معلوماتية وقانونية فيما يتعلق بنظام مكافحة الجرائم الإلكترونية ، ولكن من الضرورة الاستمرار برفع التوعية والتثقيف بشكل دوري لكافة أفراد عينة الدراسة ؛ حيث كلما تطورت وتنوعت الجرائم الإلكترونية كلما أدى ذلك إلى تحديث بالاساليب والادوات التى تزيد الوعى والحماية بشكل مستمر ليواكب كافة أنواع الجرائم الإلكترونية وأنماطها الناشئة والمستحدثة.

وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب إدراك أفراد عينة الدراسة لها كالآتي:

1) جاءت العبارة رقم (1) ، هل تعلم ما المقصود بالجريمة الإلكترونية " بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.91) من (3)

2) جاءت العبارة رقم (3) ، هل سبق لك أن وقعت ضحية لجرائم إلكترونية " بالمرتبة الثانية من حيث موافقة

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

أفراد عينة الدراسة عليها بمتوسط (2.53) من (3)
3) جاءت العبارة رقم (2) ، هل هناك فرق بين الجريمة الإلكترونية والجريمة التقليدية " بالمرتبة الثالثة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.42) من (3)

التساؤل الثاني :ما مدى الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني من وجهة نظر طلاب جامعة الملك سعود ؟

للتعرف على أسباب ضعف الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني من وجهة نظر طلاب جامعة الملك سعود ؟تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الثاني :من وجهة نظرك ماهي أسباب ضعف بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني من وجهة نظر طلاب جامعة الملك سعود ؟، وجاءت النتائج كما يوضحها الجدول الآتي:

جدول رقم (10) إجابات أفراد عينة الدراسة على المحور الثاني :من وجهة نظرك ماهي أسباب ضعف الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني من وجهة نظر طلاب جامعة الملك سعود ؟

	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعيارى	الترتيب
		النسبة	موافق	محايد	غير موافق			
1	الدخول في نظام التعلم الإلكتروني كمعلم أو كطالب آخر	ك	233	58	26	2.65	0.626	12
		%	73.5	18.3	8.2			
2	الدخول في دورة لست مسجلا بها ولكن ذلك ظهرت على صفحة التعلم الإلكتروني الخاصة بي	ك	278	26	13	2.84	0.469	8
		%	87.7	8.2	4.1			
3	دخول محاضرات الدورة رغم انسحابي من تلك الدورة	ك	302	15	0	2.95	0.213	1
		%	219	47	51			
4	تسجيل محاضرة دون إذن مدرس المقرر	ك	69.1	14.8	16.1	2.95	310.	3
		%	204	43	70			
5	تحميل محاضرة تم تسجيلها مسبقاً بواسطة الدورة المعلم ثم نشره على الإنترنت	ك	291	24	2	2.91	0.330	5
		%	64.4	13.6	22.1			
6	نشرأجزاء من محاضرة مسجلة	ك	91.8	7.6	0.6	2.81	0.494	10
		%	95.3	4.7	0			
7	استخدام محتويات مادة تعليمية على الموقع الإلكتروني	ك	290	25	2	2.70	0.611	11
		%	91.5	7.9	0.6			
8	موقع التعلم لأغراض تجارية	ك	292	21	4	2.86	0.410	6
		%	92.1	6.6	1.3			
9	تسجيل أو إلتقاط صور لشاشة الامتحان أثناء الامتحان	ك	270	33	14	2.84	0.501	9
		%	85.2	10.4	4.4			
10	أخذ لقطات من الامتحان بعد انتهائه ثم نشره	ك	249	42	26	2.85	0.460	7
		%	78.5	13.2	8.2			
11	نسخ الإعلانات من صفحة الدورة	ك	282	27	8	2.91	0.312	4

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

			2.5	8.5	89.0	%	ثم نشرها	
3	0.860	1.95	18	16	283	ك	إرسال روابط الاختبار عبر منصات التواصل الاجتماعي أو أي وسيلة اتصال أخرى	12
			5.7	5.0	89.3	%		
2	0.245	2.88	13	22	282	ك	استخدام معلومات تسجيل دخول زملائك للوصول إلى حساباتهم على التعلم الإلكتروني دون إذنهم فقط للاطلاع على معلوماتهم دون تغيير أي محتوى	13
			4.1	6.9	89.0	%		
	0.312	2.91	3	21	293	ك	الجلوس لامتحان عن بعد نيابة عن زميل	14
			2.5	24.3	73.2	%		
1	0.227	2.95	1	13	303	ك	مطالبة موقع ويب محدد بالإجابة على أسئلة الاختبار نيابة عنك	15
			0.3	4.1	95.6	%		
7	0.389	2.86	5	34	278	ك	محاولة إقتحام أو اختراق النظام باستخدام برامج خاصة	16
			1.6	10.7	87.7	%		
2	0.255	2.93	0	22	295	ك	استخدام نظام الامتحانات ودخول الاختبارات غير المخصصة لك	17
			0	6.9	93.1	%		
5	0.299	2.92	3	18	296	ك	الدخول إلى صفحة الدورة التدريبية أو مجموعة الدورة التدريبية غير المسجلة في جدول الدورة التدريبية بقصد الحصول على كلمات مرور أو ارتباط إلى المحاضرة	18
			0.9	5.7	93.4	%		
8	0.403	2.85	5	39	273	ك	الدخول إلى صفحة مقرر دراسي أو مجموعة مقرر دراسي غير مسجلة في جدولك الأكاديمي	19
			1.6	12.3	86.1	%		
4	0.281	2.92	1	23	293	ك	كتم الصوت أو تعطيله من زملائك أو المحاضر أثناء إجراء المحاضرة المتزامنة	20
			0.3	7.3	92.4	%		
6	0.291	2.91	1	25	291	ك	إرسال برامج ضارة أو برامج ضارة عبر صفحة أو مجموعة مقرر دراسي	21
			0.3	7.9	91.8	%		
3	0.267	2.93	1	20	296	ك	إرسال عدة أسئلة حول مادة الدورة من خلال صفحة الدورة أو المجموعة	22
			0.3	6.3	93.4	%		
2	0.697	2.61	39	46	232	ك	الدخول إلى صفحات أنظمة إدارة التعلم ونشر تعليقات مسيئة ضد أحد زملائك أو مدرس المقرر	23
			12.3	14.5	73.2	%		
1	0.673	2.62	34	54	229	ك	الدخول على صفحات أنظمة إدارة التعلم ونشر بعض العبارات التي قد توحي بالكراهية لزملائك أو مدرس المقرر	24
			10.7	17.0	72.2	%		
4	0.870	1.89	139	74	104	ك	إنشاء بريد إلكتروني نيابة عن	25

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

	أحد زملائك بقصد التواصل مع المحاضر نيابة عنه	%	32.8	23.3	43.8			
26	إنشاء بريد إلكتروني باسم المدرسين للتوافق مع الطلاب وذلك لضمان تواصل الطلاب معك	ك	65	69	183	1.63	0.804	5
		%	20.5	21.8	57.7			
27	مدى الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني	ك	117	73	127	1.97	0.878	3
		%	36.9	23.0	40.1			

أن هناك تجانس في موافقة أفراد عينة الدراسة أسباب ضعف الوعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني ،حيث تراوحت متوسطات موافقتهم على مدى الوعي بانشطة الجرائم الإلكترونية ما بين (2.62إلى 2.95)، وهي متوسطات تقع في الفئة الثالثة من فئات المقياس الثلاثي والتي تشير إلى" موافق " في أداة الدراسة .

وهناك تجانس ايضا فى موافقة افراد العينة حول بعض الممارسات الموجودة والتى تعتبر ضمن نطاق الجرائم الالكترونية ،حيث تراوحت متوسطات موافقتهم على مدى بانشطة الجرائم الإلكترونية ما بين (1.67إلى 2.67)، وهي متوسطات تقع في الفئة الثانية من فئات المقياس الثلاثي والتي تشير إلى" موافق "في أداة الدراسة .

وهذا مؤشر إيجابي مما يدل على أن أفرادعينة الدراسة لديهم علم ووعي بالأنشطة التى تعتبر جريمة إلكترونية متعلقة بالتعلم الإلكتروني ، ولكن من الضرورة الاستمرار برفع التوعية والتثقيف بشكل دوري لكافة أفراد عينة الدراسة ؛ حيث كلما تطورت وتنوعت الجرائم الإلكترونية كلما أدى ذلك إلى تحديث بالاساليب والادوات التى تزيد الوعى والحماية بشكل مستمر ليواكب كافة انشطة الجرائم الإلكترونية وأنماطها الناشئة والمستحدث اثناء التعلم الالكتروني.

وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب إدراك أفراد عينة الدراسة لها كالآتي:

1) جاءت العبارات رقم (3) – (4) – (15) ، كالاتى بالترتيب " دخول محاضرات الدورة رغم انسحابي من تلك الدورة " ، " تسجيل محاضرة دون إذن مدرس المقرر" ، " مطالبة موقع ويب محدد بالإجابة على أسئلة الاختبار نيابة عنك" بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.95) من (3)

2) جاءت العبارات رقم (5) – (11) – (14) – (17) – (18) ، كالاتى بالترتيب " تحميل محاضرة تم تسجيلها مسبقاً بواسطة الدورة المعلم ثم نشره على الإنترنت "، " نسخ الإعلانات من صفحة الدورة ثم نشرها " ، " الجلوس لامتحان عن بعد نيابة عن زميل " ، " استخدام نظام الامتحانات ودخول الاختبارات غير المخصصة لك" ، " الدخول إلى صفحة الدورة التدريبية أو مجموعة الدورة التدريبية غير المسجلة في جدول الدورة التدريبية بقصد الحصول على كلمات مرور أو ارتباط إلى المحاضرة " بالمرتبة الاولى بمتوسط (2.92) من (3)

3) جاءت العبارات رقم (2) – (6) – (8) – (9) – (13) – (16) – (19) ، كالاتى بالترتيب " هل هناك فرق بين الجريمة الإلكترونية والجريمة التقليدية " ، " نسخ الإعلانات من صفحة الدورة ثم نشرها " ، " نشرأجزاء من محاضرة مسجلة " ، " موقع التعلم لأغراض تجارية " ، " تسجيل أو إلتقاط صور لشاشة الامتحان أثناء الامتحان " ، " استخدام معلومات تسجيل دخول زملائك للوصول إلى حساباتهم على التعلم الإلكتروني دون إذنهم فقط للاطلاع على معلوماتهم دون تغيير أي محتوى " ، " محاولة إقتحام أو اختراق النظام باستخدام برامج خاصة " ، " الدخول إلى صفحة مقرر دراسي أو مجموعة مقرر دراسي غير مسجلة في جدولك الأكاديمي " بالمرتبة الثانية بمتوسط (2.85) من (3)

4) جاءت العبارات رقم (7) – (12) – (23) – (24) – (25) – (26) – (27) ، كالاتى بالترتيب " استخدام محتويات مادة تعليمية على الموقع الإلكتروني " ، " إرسال روابط الاختبار عبر منصات التواصل الاجتماعي أو أي وسيلة اتصال أخرى " ، " الدخول إلى صفحات أنظمة إدارة التعلم ونشر تعليقات مسيئة ضد أحد زملائك أو مدرس المقرر" ، " الدخول على صفحات أنظمة إدارة التعلم ونشر بعض العبارات التي قد توحي بالكراهية لزملائك أو مدرس المقرر " ، " إنشاء بريد إلكتروني نيابة عن أحد زملائك بقصد التواصل مع

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

المحاضر نيابة عنه " ، " إنشاء بريد إلكتروني باسم المدرسين للتوافق مع الطلاب وذلك لضمان تواصل الطلاب معك " ، " مدى الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني " ، بالمرتبة الثالثة بمتوسط (2.00) من (3)

التساؤل الثالث :ما مدى الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني من وجهة نظر طلاب جامعة الملك سعود ؟

للتعرف مدى الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني من وجهة نظر طلاب جامعة الملك سعود ؟ تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والترتيب لإجابات أفراد عينة الدراسة على المحور الثالث :من وجهة نظرك ماهي الانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ؟، وجاءت النتائج كما يوضحها الجدول الآتي:

جدول رقم (11) إجابات أفراد عينة الدراسة على المحور الثالث :من وجهة نظرك أبرز ماهي الانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ؟

	العبارة	التكرار	درجة الاستجابة			المتوسط الحسابي	الانحراف المعيارى	الترتيب
		النسبة	موافق	محايد	غير موافق			
1	أعتقدأن الجريمة الإلكترونية ليست سوى جريمة افتراضيه ليس لها أساس في الواقع	ك	233	58	26	2.65	0.626	2
		%	73.5	18.3	8.2			
2	هل يشمل قانون الجرائم الإلكترونية السعودي الجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني	ك	232	77	8	2.71	0.509	9
		%	73.2	24.3	2.5			
3	هل تعتقد أن الأنظمة والقوانين في جامعة الملك سعود (مثل مدونةالسلوك أو نظام انضباط الطلاب ...،إلخ) تضمين الجرائم الإلكترونية في التعلم الإلكتروني	ك	303	13	1	2.95	0.227	1
		%	95.6	4.1	0.3			
4	هل تعتقد أن هناك عقوبات رادعة لمن يرتكب جرائم إلكترونية في التعلم الإلكتروني	ك	278	34	5	2.86	0.389	7
		%	87.7	10.7	1.6			
5	هل تعتقد بضرورة تقديم شكوى إلى الجهات القانونية عند التعرض لجرائم إلكترونية في التعليم الإلكتروني داخل جامعة الملك سعود	ك	229	54	34	2.62	0.673	1
		%	72.2	17.0	10.7			
6	هل هناك إجراءات قانونية لتقديم شكوى عند تعرضك لجريمة إلكترونية في التعلم الإلكتروني داخل الجامعة	ك	104	61	142	1.89	0.870	4
		%	32.8	23.3	43.8			
7	هل هناك إجراءات قانونية لتقديم	ك	183	69	65	2.93	0.804	5

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

	شكوى ضد شخص يرتكب جريمة إلكترونية في التعليم الإلكتروني داخل الجامعة أو لدى الجهات القضائية المختصة	%	20.5	21.8	57.7			
8	مدى الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني	ك	291	24	2	2.91	0.330	5
		%	64.4	13.6	22.1			

يتضح من الجدول رقم (11) ما يأتي:
أن هناك تجانس في موافقة أفراد عينة الدراسة على مدى الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ،حيث تراوحت متوسطات موافقتهم على مدى الوعي لديهم بالانظمة والقوانين المرتبطة بالجرائم الالكترونية المتعلقه بالتعلم الالكتروني ما بين (2.86إلى 2.95)، وهي متوسطات تقع في الفئة الثالثة من فئات المقياس الثلاثي والتي تشير إلى" موافق "في أداة الدراسة .
وهناك تجانس ايضا فى موافقة افراد العينة حول بعض القوانين والانظمة التى تنظم وتحدد نطاق الجرائم الالكترونية ،حيث تراوحت متوسطات موافقتهم على الوعي بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني (2.62إلى 2.71)، وهي متوسطات تقع في الفئة الثانية من فئات المقياس الثلاثي والتي تشير إلى" موافق "في أداة الدراسة .
وهذا مؤشر إيجابي مما يدل على أن أفرادعينة الدراسة بالانظمة والقوانين الجرائم الالكترونية المتعلقه بالتعلم الالكتروني ، ولكن من الضرورة الاستمراربالتعريف بهذه القوانين والانظمة بشكل دوري لكافة أفراد عينة الدراسة ؛ حيث كلما تطورت وتنوعت الجرائم الإلكترونية كلما أدى ذلك إلى شن القوانين وفرض الانظمة الصارمة لمواجهه الجرائم الالكترونية بصفه عامة والمتعلقة بالتعلم الالكتروني بصفه خاصة
وفيما يلي ترتيباً تنازلياً لعبارات المحور حسب إدراك أفراد عينة الدراسة لها كالآتي:

1) جاءت العبارات رقم (3) – (7) – (8) ، كالاتى بالترتيب " هل تعتقد أن الأنظمة والقوانين في جامعة الملك سعود (مثل مدونةالسلوك أو نظام انضباط الطلاب ...،إلخ) تضمين الجرائم الإلكترونية في التعلم الإلكتروني " ، " هل هناك إجراءات قانونية لتقديم شكوى ضد شخص يرتكب جريمة إلكترونية في التعليم الإلكتروني داخل الجامعة أو لدى الجهات القضائية المختصة " ، " مدى الوعي بالجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني " بالمرتبة الأولى من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (2.92) من (3)
2) جاءت العبارات رقم (1) – (2) – (4) – (5) ، كالاتى بالترتيب " أعتقدأن الجريمة الإلكترونية ليست سوى جريمة افتراضيه ليس لها أساس في الواقع "، " هل يشمل قانون الجرائم الإلكترونية السعودي الجرائم الإلكترونية المتعلقة بالتعلم الإلكتروني " ، " هل تعتقد أن هناك عقوبات رادعة لمن يرتكب جرائم إلكترونية في التعلم الإلكتروني " ، هل تعتقد بضرورة تقديم شكوى إلى الجهات القانونية عند التعرض لجرائم إلكترونية في التعليم الإلكتروني داخل جامعة الملك سعود " ،بالمرتبة الثانية بمتوسط (2.65) من (3)
3) جاءت العبارة رقم (6) ، هل هناك إجراءات قانونية لتقديم شكوى عند تعرضك لجريمة إلكترونية في التعلم الإلكتروني داخل الجامعة " بالمرتبة الثالثة من حيث موافقة أفراد عينة الدراسة عليها بمتوسط (1.89) من (3)

النتائج والتوصيات

أولاً :النتائج:

أسفرت الدراسة إلى مجموعة من النتائج، يمكن إجمالها فيما يلي:
1) توصلت الدراسة إلى أن مستوى الوعي بالجرائم الإلكترونية المذكورة بنظام مكافحة الجرائم الإلكترونية السعودي قد بلغ درجة مرتفعة لدى أفراد عينة الدراسة ، بمتوسط حسابي قدره
2) بينت احصائيات الدراسة أن أفراد عينة الدراسة لديهم معرفة وثقافة قانونية عالية فيما يتعلق بنظام

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

مكافحة جرائم الإلكترونية السعودي.

3) كشفت الدراسة أسباب ضعف الوعي بنظام مكافحة جرائم الإلكترونية السعودي حسب وجهة نظر أفراد عينة الدراسة

4) قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم الإلكترونية من خلال الاطلاع عليه ومعرفة مدى أهميته.

5) قلة برامج التوعية والاثراء بالجرائم الإلكترونية وكيفية التعامل معها وفق التشريعات المحلية.

6) -عدم وضوح صياغة الألفاظ والعبارات للنظام بشكل مناسب لكافة فئات المجتمع.

7) -عدم تثقيف أفراد المجتمع بنظام مكافحة الجرائم الإلكترونية من قبل الجهات الأمنية المختصة.

8) صعوبة فهم المواد المنصوصة بنظام مكافحة جرائم الإلكترونية وكيفية الأخذ بها.

9) جهل بعض أفراد المجتمع بأن الفضاء المعلوماتي لديه قوانين وتشريعات محلية.

10) عدم حل المشكلة الأساسية التي أدت إلى ارتكاب الجريمة الإلكترونية .

11) تبين من الدراسة أن من أسباب ضعف الوعي بنظام مكافحة جرائم الإلكترونية السعودي الأكثر أثراً حسب وجهة نظر أفراد العينة هو قلة اهتمام أفراد المجتمع بنظام مكافحة جرائم الإلكترونية من خلال الاطلاع عليه ومعرفة مدى أهميته.

12) كشفت الدراسة عن أبرز طرق المكافحة والوقاية من الجرائم الإلكترونية في ظل التحول الرقمي تماشياً مع رؤية 2030 حسب وجهة نظر أفراد عينة الدراسة ، وتتمثل على النحو الآتي:

- تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاخت ا رقات الإلكترونية.
- مواكبة التطو ا رت المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
- زيادة برامج التوعية والاثراء بالجرائم الإلكترونية وكيفية التعامل معها وفق التشريعات المحلية.
- تثقيف أفراد المجتمع بالأساليب الصحيحة والآمنة عند استخدام الشبكة الإلكترونية.
- تثقيف أفراد المجتمع بضرورة إبلاغ الجهات الأمنية المختصة في حال التعرض لجريمة معلوماتية.
- تأسيس وحدة أمنية خاصة لمكافحة الجرائم الإلكترونية والحد منها.
- تشجيع الهيئات على استخدا م التشفير الوطني للبيانات للمساهمة في حماية البيانات والأنظمة والشبكات الوطنية.
- لقيام بمبادرا ت تقدم دو ا رت تدريبية وورش تعليمية لمكافحة الجرائم الإلكترونية مجاناً لكافة ش ارئح المجتمع.
- تفعيل تقنية التوقيع الالكتروني وتطبيقها في كافة الخدمات الحكومية وغيرها، لرفع مستوى الموثوقية ومنع إساءة الاستخدام والاحتيال في التعاملات الالكترونية.
- استخدام تقنية Blockchain للحد من التلاعب بالهوية.
- توعية أفراد المجتمع بالجرائم الإلكترونية وأنظمة مكافحتها عن طريق برامج، وتطبيقات التواصل الاجتماعي.
- تأسيس منصة خاصة بالجرائم الإلكترونية يتم من خلالها رفع العقوبات التي أخذت صفة قطعية ونشرها؛ والتشهير بالمجرم المعلوماتي.
- إدراج اللوائح والقوانين في حساب المواطن عبر بوابة ابشر وأخذ تعهد بعد كل ستة أشهر ليضل المواطن على وعي مستمر.

13) بينت احصائيات الدراسة أن تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية تحتل المرتبة الأولى من طرق مكافحة الجرائم الإلكترونية حسب وجهة نظر أفراد العينة.

14) أظهرت الدراسة إلى أن مستوى المعرفة والوعي بأدوات الإبلاغ عن الجرائم الإلكترونية في المملكة العربية السعودية قد بلغ درجة متوسطة لدى أفرادعينة الدراسة

ثانياً :التوصيات:

في ضوء النتائج التي توصلت إليها الدراسة توصي بالآتي:

1) ضرورة تطوير وتحديث نظام مكافحة الجرائم الإلكترونية السعودي بشكل مستمر ليواكب كافة أنواع الجرائم الإلكترونية وأنماطها الناشئة والمستحدثة.

2) ينبغي على الجهات المختصة القيام بمبادرات توعوية تساهم في توعية أفراد المجتمع بما يتعلق بالجرائم

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

الإلكترونية وأنظمة مكافحتها بشكل دوري ومستمر لرفع مستوى ثقافة المجتمع.

3) يجب على الجهات المختصة الأخذ بالاعتبار بأبرز طرق المكافحة والوقاية من الجرائم الإلكترونية في ظل التحول الرقمي تماشياً مع رؤية 2030 للملكة .

4) تثقيف وتوعية أفراد المجتمع بأدوات الإبلاغ عن الجرائم الإلكترونية في المملكة العربية السعودية باعتماد طرق وأساليب متنوعة كمقاطع الفيديو، والمطويات، والنشرات... الخ.

5) ضرورة توحيد طرق مكافحة الجرائم الإلكترونية والوقاية منها؛ للحد من انتشار الجرائم الإلكترونية .

6) أهمية إدراج موضوع الجرائم الإلكترونية ضمن المقررات الدراسية التي لها علاقة بها؛ وذلك لإكساب الطلاب والطالبات مهارات الحماية من مخاطر الجرائم الإلكترونية وكيفية التعامل معها وفق التشريعات المحلية.

7) إجراء دراسات علمية لمعرفة مستوى وعي الطلبة بنظام مكافحة جرائم الإلكترونية ولإثراءالإنتاج الفكري العربي.

8) إجراء دراسات علمية متخصصة لمعرفة جهود المملكة العربية السعودية في مكافحة الجرائم الإلكترونية .

المراجع

1. الرشيدي ع & ,.المهداوي . ع. . (2023). مستوى الوعي بنظام مكافحة الجرائم المعلوماتية لدى طلاب الجامعة .*المجلة العربية للدراسات الأمنية*.51-63 ,(1)*39* .

2. الإدارة العامة للأمن السيبراني بجامعة الملك خالد ، (2023) (الجرائم المعلوماتية) ، https://www.kku.edu.sa/ar/node/101084

3. رجب، سها عيد. (2023). الجرائم الإلكترونية ووعي الشباب بانتهاكها لخصوصية الفرد .*حوليات آداب عين شمس، مج51* ، 332 – 299

4. Adams, A., Blanford, A., 2003. Security and Online Learning: to Protect and Prohibit. In: Usability Evaluation of Online Learning Programs. IGI Global, pp. 331–359.

5. Adnan, M., Anwar, K.J.O.S., 2020. Online learning amid the COVID-19 pandemic: students' perspectives. Online Submission 2 (1), 45–51.

6. Al-Bdour, M., AlShawabkeh, M.a., Alni'mat, A., AlRyalat, S.A., Abuameerh, O., 2022. Students' perceptions of e-learning in medical faculties in Jordan during the COVID19 pandemic. Int. Med. J. 29 (2). Algahtani, A., 2011. Evaluating the Effectiveness of the E-Learning Experience in Some Universities in Saudi Arabia from Male Students' Perceptions. Durham University.

7. Almosa, A., 2002. Use of Computer in Education. Future Education Library, Riyadh, Saudi Arabia.

8. Almosa, A., Almubarak, A., 2005. E-Learning Foundations and Applications. Riyadh, Saudi Arabia.

9. Alsoud, A.R., Harasis, A.A., 2021. The impact of covid-19 pandemic on student's elearning experience in Jordan. J. Theor. Applied Electr. Comm. Res. 16 (5), 1404–1414.

10. Alwi, N.H.M., Fan, I.-S., 2010. E-learning and information security management. International Journal of Digital Society 1 (2), 148–156. Arkorful, V., Abaidoo, N., 2015. The role of e-learning, advantages and disadvantages of its adoption in higher education. Int. J. Instr. Technol. Dist. Learning 12 (1), 29–42.

11. Aydın, C.H., Tasci, D., Society, 2005. Measuring readiness for e-learning: reflections from an emerging country. J. Educ. Technol. 8 (4), 244–257. Balkin, J.,

DOI: https://doi.org/10.33193/JEAHS.33.2024.459
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., Zarsky, T., 2007. Cybercrime: Digital Cops in a Networked Environment, 4. NYU Press.

12. Barakat, M., Farha, R.A., Muflih, S., Ala'a, B., Othman, B., Allozi, Y., Fino, L., 2022. The era of E-learning from the perspectives of Jordanian medical students: a crosssectional study. Heliyon 8 (7).
13. Bele, J.L., Dimc, M., Rozman, D., Jemec, A.S., 2014. Raising Awareness of Cybercrime– The Use of Education as a Means of Prevention and Protection. ERIC.
14. Borotis, S., Poulymenakou, A., 2004. E-learning readiness components: key issues to consider before adopting e-learning interventions. In: Paper Presented at the E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education.
15. Campbell, L., 2004. What does the "e" stand for. Department of Science Mathematics Education. The University of Melbourne, Melbourne.
16. Carlisle, L., 2020. Investing in E-Learning Remains a Priority for UNHCR Jordan. Retrieved from. https://www.unhcr.org/jo/13661-investing-in-e-learning-remainsa-priority-for-unhcr-jordan.html.
17. Chandarman, R., Van Niekerk, B., 2017. Students' cybersecurity awareness at a private tertiary educational institution. The African J. Inform. Communication 20, 133–155.
18. Crawford, J., Butler-Henderson, K., Rudolph, J., Malkawi, B., Glowatz, M., Burton, R., Lam, S., 2020. COVID-19: 20 countries' higher education intra-period digital pedagogy responses. Journal of Applied Learning Teaching 3 (1), 1–20.
19. Cybercrime Law, 27 C.F.R. (2015). Fawaz, M., Samaha, A., 2021. E-learning: Depression, Anxiety, and Stress Symptomatology Among Lebanese university Students during COVID-19 Quarantine. In: Paper Presented at the Nursing Forum.
20. Gandhi, V.K., Thanjavur, T.N.S.I., 2012. An overview study on cyber crimes in internet. J. Inf. Eng. Appl. 2 (1), 1–5.
21. Gonzalez, T., De La Rubia, M., Hincz, K.P., Comas-Lopez, M., Subirats, L., Fort, S., Sacha, G., 2020. Influence of COVID-19 confinement on students' performance in higher education. PLoS One 15 (10), e0239490.
22. Keller, C., Cernerud, L., 2002. Students' perceptions of e-learning in university education. J. Educ. Media 27 (1-2), 55–67.
23. Kerr, O.S., 2003. Cybercrime's scope: interpreting access and authorization in computer misuse statutes. NYUL Rev 78, 1596.
24. Kidd, T.T., 2009. Online Education and Adult Learning: New Frontiers for Teaching Practices: New Frontiers for Teaching Practices. IGI Global. King,
25. C.G., Guyette Jr., R.W., Piotrowski, C., 2009. Online exams and cheating: an empirical analysis of business students' views.
26. J. Educ. Online 6 (1), n1. Kshetri, N., 2010a. Cloud computing in developing economies. Computer 43 (10), 47–55.
27. Kshetri, N., 2010b. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Springer Science & Business Media.
28. Kunz, M., Wilson, P., 2004. Computer Crime and Computer Fraud.
29. LaRose, R., Gregg, J., Eastin, M., 1998. Audiographic telecourses for the Web: an

DOI: https://doi.org/10.33193/JEAHS.33.2024.459
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

experiment. J. Computer-Mediated Commun. 4 (2), JCMC423.
30. Lewis, J.R., 2018. Is the report of the death of the construct of usability an exaggeration? J. Usability Studies 14 (1), 1–7.
31. Liguori, E., Winkler, C., 2020. From Offline to Online: Challenges and Opportunities for Entrepreneurship Education Following the COVID-19 Pandemic. In: Entrepreneurship Education Pedagogy, 3. SAGE Publications Sage CA, Los Angeles, CA, pp. 346–351.
32. Mailizar, A., Abdulsalam, M., Suci, B., 2020. Secondary school mathematics teachers' views on e-learning implementation barriers during the COVID-19 pandemic: the case of Indonesia.
33. Eurasia J. Math. Sci. Technol. Educ. 1–9. Maimon, D., Louderback, E.R., 2019. Cyber-dependent crimes: an interdisciplinary review. Annual Review of Criminology 2, 191–216.
34. Marino, T., Eager, M., Draxler, T., 2000. Learning Online: A View from Both Sides. The National Teaching & Learning Forum.
35. Ndume, V., Tilya, F., Twaakyondo, H., 2008. Challenges of adaptive elearning at higher learning institutions: a case study in Tanzania. Int. J. Comput. Intell. Res. 2 (1), 47–59. Petee, T.A.
36. Corzine, J., Huff-Corzine, L., Clifford, J., Weaver, G., 2010. Defining "cybercrime": issues in determining the nature and scope of computer-related offenses. Futures Working Group 5, 6–11.
37. Poonia, A.S., Dangayach, G., Bhardwaj, A., 2012. Integrating and teaching cyber ethics in eLearning environment. Int. J. Comput. Integrated Manuf. 20, 1–6.
38. Raheem, B.R., Khan, M.A., 2020. The role of e-Learning in COVID-19 crisis. Int. J. Creat. Res. Thoughts 8 (3), 3135–3138.
39. Reeves, T.C., 2000. Alternative assessment approaches for online learning environments in higher education. J. Educ. Comput. Res. 23 (1), 101–111.
40. Rogers, C.F., 2006. Faculty perceptions about e-cheating during online testing. J. Comput. Sci. Colleges 22 (2), 206–212.
41. Rossi, P., 2009. Learning environment with artificial intelligence elements. J. e Learn. Knowl. Soc. 5 (1), 67–75.
42. Rowe, N.C., 2004. Cheating in online student assessment: beyond plagiarism. Online J. Dist. Learn. Adm. 7 (2).
43. Salahshouri, A., Eslami, K., Boostani, H., Zahiri, M., Jahani, S., Arjmand, R., Dehaghi, B.F., 2022. The university students' viewpoints on e-learning system during COVID-19 pandemic: the case of Iran. Heliyon 8 (2), e08984. Shahroury, F.R., 2022. E-LEARNING during COVID-19 epidemic: experience of a university from Jordan. Acad. Strat.
44. Manag. J. 21 (S4). Srivastava, A., Sinha, S., 2013. Information security through e-learning using VTE. Int. J. Electron. Comput. Sci. Eng. 2 (18), 528–531.
45. Toquero, C.M., 2020. Challenges and opportunities for higher education amid the COVID19 pandemic: the Philippine context. Pedagogical Res. 5 (4). H.Y.
46. Ayyoub et al. Heliyon 8 (2022) e10897 10 Underwood, J., Szabo, A., 2003. Academic offences and e-learning: individual propensities in cheating. Br. J. Educ.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.33.2024.459
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (33) March 2024
العدد (33) مارس 2024

Technol. 34 (4), 467–477.

47. Urdan, T.A., Weggen, C.C., 2000. Corporate Elearning: Exploring a New Frontier. Venter, I.M., Blignaut, R.J., Renaud, K., Venter, M.A., 2019. Cyber security education is as essential as “the three R's”. Heliyon 5 (12), e02855.
48. Watkins, R., Leigh, D., Triner, D., 2004. Assessing readiness for e-learning. Perform. Improv. Q. 17 (4), 66–79.
49. Wentling, T., Waight, C., Gallaher, J., Fleur, J., Wang, C., Kanfer, A., 2000. E-Learning: A Review of Literature’Knowledge and Learning Systems Group. National Center for Supercomputing Applications, University of Illinois, pp. 1–73.
50. Zeitoun, H., 2008. E-learning: concept, issues, application, evaluation. In: Riyadh. Dar Alsolateah Publication. Zhong, R., 2020. The Coronavirus Exposes Education’s Digital divide, 18. The New Yor