

إدارة المخاطر

أثر المخاطر التقنية على التعليم الإلكتروني في الجامعات السعودية

مهند الشبيلي (20222005886)

وائل حكيم (20222006199)

خالد محمود (20222005875)

عيسى المطيري (20212005041)

سلطان منصور (20212005038)

عبد الله القحطاني (20222005858)

اكتمال الجيزاني (2021206584)

نايف الرشيد (20212005057)

ملاك السعدون (20222005691)

يوسف بالبيد (20212005218)

المشرف: د/وليد سليمان

2022 م

1. مقدمة:

كما يعلم الجميع بأنه لا يوجد أي بيئة تقنية لا تخلو من المخاطر، ويختلف تأثير هذه المخاطر حسب نوع الخطر ولعلنا نركز في هذه الدراسة على المخاطر التي تؤثر على التعليم الإلكتروني والذي بطبيعة الحال شهد تطورات كبيرة خلال الفترات الماضية حاله أي مجال اعتمد على التقنية واستخدام شبكة الانترنت، وكما يظهر بأن المؤسسات التعليمية ذات طابع التعليم التقليدي المعروف اتجهت للتعليم الإلكتروني إما لبعض من موادها التعليمية أو جزء منها خاصة ذات الطابع النظري، بل وظهرت مؤسسات تعليم وتدريب تقوم بالدور التعليمي كاملاً بشكل إلكتروني خاصة وأن ما ساعد التعليم الإلكتروني كثيراً في توسعه وانتشاره هو سهوله الحصول عليه والوصل له مما يسهم في منح المتعلم المرونة في الوقت والمكان ويستطيع التعلم بكل سهوله وبتكاليف أقل كما يمنح المتعلم البحث والوصول لمواضيع مختلفة في شتى العلوم وبذلك أصبح يحظى باهتمام الكثير من الراغبين في التعليم و التعلم، ولكن كون هذا النوع من التعليم يعتمد على التقنية فمن الطبيعي أن يكون عرضةً للمخاطر التقنية، حيث جاءت الدراسة لبحث ودراسة أكثر المخاطر التقنية التي قد يتعرض لها قطاع التعليم الإلكتروني والتي قد تؤثر على ضمان استمرارية عمل وبحث أفضل الطرق للتخفيف من هذه المخاطر أو إنهاؤها.

2. مشكلة الدراسة

نظراً لانتشار التهديدات الإلكترونية والتي هي بطبيعة الحال هي مخاطر تقنية والتي يحدث انتشارها وكثرتها أثراً على البيئة التقنية التي من خلالها يتم تقديم عملية التعليم الإلكتروني والتي قد تتعرض لها وهذا يؤثر على أعمالها وموثوقيتها وقد تكون ذا أثر عالي قد يتسبب في انقطاع العملية التعليمية لفترة غير مسموح بها في المؤسسات التعليمية التي تقدم هذا النوع من التعليم، فتوجب لزماً بحث المشكلة وإيجاد الحلول للمخاطر التقنية التي تؤثر على ضمان استمرار تقديم عملية التعليم الإلكتروني في كل وقت.

3. أهمية الدراسة:

يتزامن البحث مع رؤية ٢٠٣٠ واهتمام المملكة العربية السعودية لتنفيذ الحكومة الإلكترونية في كافة القطاعات ومع توجه معظم مؤسسات التعليم لتطبيق التعليم الإلكتروني، تتجلى أهمية الدراسة في مدى التخفيف والحد من المخاطر التقنية التي قد تتعرض لها الجامعات السعودية التي من خلالها يتم تقديم عملية التعليم الإلكتروني ومساهمتها في جودة الأداء واستمرارية العمل للمؤسسات التي تتبنى وتقدم التعليم الإلكتروني.

4. أهداف الدراسة

- 1- التعرف على أكثر الطرق أو الإجراءات المناسبة للحد من المخاطر التقنية التي تؤثر على استمرارية الأعمال.
- 2- إيجاد حلول لتخفيف المخاطر التقنية التي قد تتعرض لها مؤسسات التعليم الإلكتروني.
- 3- رفع نسبة ضمان استمرارية الأعمال وخصوصية بيانات المستخدمين.
- 4- إيجاد وصياغة سياسات وإجراءات تحدد الإطار العام والخاص للتعليم الإلكتروني.

5- أسئلة الدراسة

- 1- ماهي المخاطر التقنية ذات التأثير المرتفع؟
- 2- ما مدى إيجاد حلول تقنية متاحة للاستخدام لضمان استمرارية الأعمال؟
- 3- ماهي الأنظمة الإلكترونية التي تساعد الطلاب وتوفر سبل الاستمرارية للتعلم؟
- 4- ماهي التجارب المثل في أنظمة الفصول الافتراضية؟

6- الدراسات السابقة والإطار النظري

الدراسة الأولى:

الدكتور أحمد الدماس مستشار تقنية الاتصالات والمعلومات "إن السعودية هي أولى دول الشرق الأوسط في التعرض للهجمات الإلكترونية، تليها الإمارات"، مشيراً إلى أن الهجمات وصلت في 2014 إلى 43 مليون هجمة، وهذا العدد زاد بمعدل الضعف خلال العامين التاليين.

الأهداف:

يتطلب منح الأمن السيبراني عناية أكبر لدى الجهات والشركات في المملكة.

المتغير المستقل:

وأشار إلى أن الدراسات تؤكد زيادة استخدام المجتمع السعودي للإنترنت، حيث يستخدم 50 في المائة من السعوديين.

المتغير التابع:

أن الأمن التقني والإلكتروني يعمل جنباً إلى جنب مع الأمن الفكري.

منهجية الدراسة:

وبين أن البرنامج بدأ بتعيين ممثل له في كل مدرسة ليكون حلقة وصل بين المدارس وبين تطبيق أهداف واستراتيجية البرنامج وحماية طلاب المدارس وتحصينهم ضد هجمات الأعداء التقنية والفكرية.

اهم النتائج والتوصيات:

وجود سبعة أبعاد للأمن السيبراني هي: القانوني والتقني والتنظيمي والتعاون الدولي والتوعية، وبناء القدرات والتصدي للهجمات الاستباقية، لافتاً إلى أن هذه الأبعاد يجب أن يتم الاهتمام بتنفيذها بنفس القدر من الأهمية.

الدراسة الثانية: وزارة التعليم والعطويوي 2020

الأهداف:

بداية جائحة كورونا تم العمل على خلق بيئات تعلم عن بُعد تدعم التعليم العام، ومتابعة سير العملية التعليمية.

المتغير المستقل:

عدد الاختبارات المسندة للطلاب والطالبات عن بُعد خلال العام الدراسي 2020 تجاوزت 107 ملايين اختبار يومياً، بمتوسط حل يقارب 700 مليون، أما عدد الواجبات المسندة للطلاب والطالبات فبلغ 83.2 مليون واجب يومياً، بما يفوق 12 مليار متوسط الحل.

المتغير التابع:

ورغم هذه الأرقام المليونيرة، فإن بعض طلاب التعليم العام لم يلتحقوا بمنصة «مدرستي»، وهو ما أرجعته وزارة التعليم في تقريرها الإحصائي لعدة أسباب منها عدم توفر اتصال بشبكة الإنترنت، أو تعذر الوصول إلى قنوات «عين» التعليمية لأسباب صحية أو نفسية أو تقنية.

منهجية الدراسة:

يشير أستاذ تقنية التعليم إلى اختلاف بين إيجاد الحلول المناسبة للآزمات وتقليل الآثار منها باستخدام الأدوات الإلكترونية والتعليم عن بعد. ويشرح ذلك بالقول: «هذا النوع تم التخطيط له بطريقة صحيحة من جميع الاحتياجات التي تطلبها البيئة الإلكترونية عن بعد، والمتعلم والمعلم، وفي حالة الفشل في تحقيق الأهداف يكون فشل في التعليم عن بعد.

أهم النتائج والتوصيات:

تعتبر الوزارة حققت نتائج رغم أن العالم لم يكن لديه القدرة على التنبؤ بآثارها لانعدام المعلومات المتوفرة لديه، لأن الطالب على الأقل لم يكن بعيداً عن العملية التعليمية.

الدراسة الثالثة: المجلة الدولية لأمن شبكات الحاسوب والاتصالات؛ دبي 2020

الأهداف:

قد تناولت الهجومات السيبراني في السعودية بهدف مكافحة هذه الهجمات على أجهزة الكمبيوتر والشبكات.

المتغير المستقل:

الهجمات السيبرانية.

المتغير التابع:

تلف الأنظمة أو الشبكات.

منهجية الدراسة:

الجدول الزمني للهجمات التي تشهدها هذه البرامج الضارة.

اهم النتائج والتوصيات:

النقص في البحث أو التحقيق العلمي في الهجمات الإلكترونية على المملكة العربية السعودية والبحث في منهجيات وهياكل الامن السيبراني للدفاع في المستقبل.

الدراسة الرابعة: الفئار للإعلان 2015

الأهداف:

قد تناولت الهجوم السيبراني في السعودية بهدف مكافحة هذه الهجمات على أجهزة الكمبيوتر والشبكات.

المتغير المستقل:

الهجمات السيبرانية.

المتغير التابع:

تلف الأنظمة أو الشبكات.

منهجية الدراسة:

تقارير جديد ومقابلات مع خبراء.

أهم النتائج والتوصيات:

تحتاج الجامعات العربية إلى حماية أفضل من المخاطر التي جلبها العصر الرقمي معها.

الدراسة الخامسة:

وجدان الجهني ونزار الفاضل ومسام جراجرة (جامعة فهد بن سلطان، تبوك، السعودية). و مواهب غازميسيد ،

جامعة تبوك، السعودية. 2021

الأهداف:

قياس مستوى الوعي بالأمن السيبراني لدى طلاب جامعة المملكة العربية السعودية بهدف الوعي بالوضع السيبراني لإدراك النشاط الضار، وفهم تأثير ونوع التهديد، والتنبؤ بالعواقب المستقبلية والقدرة على ادارة المخاطر المترتبة على ذلك.

المتغير المستقل:

الجنس والموقع والقسم.

المتغير التابع:

مستوى الوعي بالأمن السيبراني.

منهجية الدراسة:

استخدم الباحث المنهج الوصفي بالأسلوب الإسباني نظراً لملائمته لطبيعة البحث.

أهم النتائج والتوصيات:

تشير نتائج الدراسة إلى أن الطلاب لديهم مستويات متوسطة من الوعي فيما يتعلق بمفاهيم الأمن السيبراني والتوصية بدعم البرامج التدريبية والتوعوية وكذلك اعتماد كافة إجراءات السلامة اللازمة من قبل الأكاديميين وموظفي المؤسسة لتعزيز أمن وسلامة بياناتهم وتطوير نهج استباقي نحو تعزيز الأمن السيبراني من خلال توعية الموظفين بالأشكال الجديدة للتهديدات الأمنية والتدابير التي يجب اتباعها عند تحديد نشاط مشبوه.

7- المنطلقات النظرية للدراسة

تعددت البحوث والدراسات ووفقا لمعظم الابحاث يقابل ايجابيات التعليم الالكتروني تأتي المخاطر الأمنية الأساسية ممثلة في التهديدات السيبرانية الأساسية مثل البرامج الضارة ومشاركة الطرف الثالث حيث أصبحت التهديدات أكثر ذكاء وعدم قدرة بعض أجهزة التعلم الالكتروني عن الدفاع عن نفسها حيث انه وفقا للإحصاءات "تحتوي 42٪ من التطبيقات على برامج ضارة بينما يمكن أن تكون 6٪ هي سبب المخاطر" (7) مع الحاجة لضرورة التعامل مع هذه المخاطر لتجنب الخسارة.

ومن الأمثلة على البرامج الضارة التي يوجهها التعليم عبر الإنترنت وتهديداتها، الفيروسات والديدان وبرامج الفدية و Trojan horses, keyloggers, rootkits وبرامج التجسس والبرامج الإعلانية. في الواقع، ان البرامج الضارة الأكثر شيوعا التي تؤثر على التعليم عبر الإنترنت هي برامج المخاطر والبرامج الإعلانية عند استخدام الكثير من الطلبة لأجهزة الكمبيوتر المحمولة للتعليم والعمل عبر الإنترنت أو لأغراض شخصية ، حيث هناك احتمال كبير لتأثر هذه الاجهزة بالبرامج الضارة ، مما يتسبب في مشكلات مختلفة مثل التأثير على قابلية تشغيل أجهزة الكمبيوتر وشبكات الكمبيوتر ، وفشل الأجهزة ، وفقدان البيانات أو سرقتها، وبالتالي يحتمل أن يؤثر سلبا على جودة تجربة التعلم عبر الإنترنت ، إضافة لهجمات هجمات القرصنة والحرمان من الخدمة، والغاء شبكة النت وجعلها غير قابلة للوصول إلى الطلبة. كما يشكل الانتحال والاحتيال وسرقة البيانات مشاكل لمستخدمي التعليم عبر الإنترنت .

وغالبا ما يستخدم المحتالون الانتحال على هيئة بوابات مزيفة كمصدر معروف لدى المتلقي، للحصول على إذن وتفصيل عن الطلاب مثل كلمات المرور وغيرها من المعلومات الحساسة. وقد يؤدي ذلك إلى سرقة البيانات، وتحديد البيانات الشخصية وبيانات الطلاب، والتي يمكن أن تكون ضمن نطاق لوائح الخصوصية مما يؤثر على سرية ونزاهة وسمعة التعليم عبر الإنترنت، كما يتوجب على الجامعات عمل التدابير اللازمة لضمان تأمين شبكة الإنترنت.

واخيرا وليس اخرا اود التنويه لقضية مهمة الا وهي اجراء الامتحانات بشكل صحيح عبر الإنترنت في التعليم عن بعد يعد امرا بالغ الأهمية لضمان صحة شهادة التعلم حيث ان أحد الحلول لإجراء الامتحانات عبر الإنترنت هو استخدام مراقب عبر الإنترنت لضمان عدم غش الطلاب. ومع ذلك، فإن هذا الأمر يمثل تحديا، نظرا لأن أحدث التقنيات مثل الساعات الذكية والنظارات الذكية تسهل على الطلاب الغش في الاختبارات وللحفاظ على سلامة أسئلة الامتحان، من الضروري التأكد من أن الطلاب لا يشاركون تفاصيل الامتحان مع زملائهم في الفصل وغالبا ما تستخدم الجامعات برامج المراقبة عبر الإنترنت. ومع ذلك، يجب إجراء دراسات صارمة لضمان فعالية هذه البرامج في منع الغش.

"يقول 47 % من قادة الأعمال إن الخطأ البشري، مثل فقدان العرضي لجهاز أو مستند، أدى إلى خروقات البيانات داخل مؤسساتهم" (8)

لقد أزلت ثورة التعليم الالكتروني العديد من الحواجز المتعلقة بالعمر والجنس والمكان والطبقة الاجتماعية التي كانت موجودة سابقا في التعليم .

ومع ذلك، هناك عيوب أيضا، تشمل الأمان والخصوصية والقضايا المتعلقة بهما. إن وجود الضوابط المناسبة فيما يتعلق بمصادقة المستخدم وتفويضه، واستخدام برامج مكافحة الفيروسات، واستخدام المسح الضوئي عن بعد للأنظمة، وتنفيذ تدريب المستخدم النهائي يمكن أن يساعد في تقليل المخاطر السيبرانية المتعلقة بالتعلم عن بعد عبر الإنترنت وضمان سلامة وسرية الدورات الدراسية وإنجاز الطلاب والمعلومات الشخصية. (9)

8- المنهجية وطرق البحث

اعتمدت الدراسة الحالية المنهج الوصفي لملاءمته لأهداف وطبيعة الدراسة.

9- أدوات الدراسة

تم اعتماد أداة الاستبانة بالأسئلة المفتوحة كأداة لجمع بيانات الدراسة وقد تم تصميمها بالاستفادة من الإطار النظري.

10- مجالات الدراسة

المجال المكاني :

سوف يتم تطبيق هذا البحث على اساتذة وطلاب الجامعات الالكترونية في المملكة العربية السعودية.

المجال البشري:

سوف يتم توزيع استبانة البحث على الطلاب والاساتذة بجامعة الجميع الذكية في مدينة الرياض وعددهم ٥٠ شخص حيث سوف نقوم بمسح شامل للجامعة لمعرفة المخاطر التقنية التي واجهتهم وتسبب خطر على الجامعة وعدم استمرارية الاعمال .

المجال الزمني:

سوف تجري الدراسة الاستطلاعية والأساسية في فترة 2022/10/18 الى 2022/12/30

وقد اجريت الدراسة الاستطلاعية في الفترة من 2022/10/29 الى 2022/11/05

اجريت الدراسة الأساسية في فترة من 2022/11/06 الى 2022/12/21

11- المخاطر التقنية

- 1- الإختراق (Hacking): كسر الحواجز والجدر النارية الواقية للخوادم والأجهزة.
- 2- الفايروسات: برامج ضارة تحدث تلفاً أو فقداً للمعلومات والبيانات
- 3- الدُخول غير المُصرَّح به (unauthorized Access): الدخول بطريقة غير مصرح بها إلى الأنظمة أو البرامج
- 4- استخدام النُسخ غير الأصلية من البرامج: استخدام نسخ غير مصرَّح بها من البرامج أو الأنظمة التي تخدم العمل، ما قد يُسبِّب التوقُّف في لحظة ما خلال العمل، أو عدم المقدرة على إجراء أعمال على تلك البرامج، بسبب توقُّفها لأنها غير مُرَخَّصة.
- 5- التَّعديل غير المُصرَّح به للبيانات أو المعلومات: الحصول على اسم المستخدم او كلمة السر بطريقة غير مشروعة ومن ثم تعديل البيانات وربما يكون ذلك التعديل عن طريق استغلال موقع محدد لتعديل البيانات والمعلومات .
- 6- دقَّة البيانات والمعلومات وتوافقها وتكاملها: يتمثّل هذا الخطر في إدخال بيانات غير دقيقة أو خاطئة ما يسبِّب مخرجات غير دقيقة وخاطئة، كذلك عدم توافق البيانات المُدخلة وعدم تكاملها.
- 7- أعطال الأجهزة أو البرامج: تعطل الأجهزة الرئيسة بالجهة، أو أحد البرامج أو الانظمة المرتبطة بها، مما يتسبب في انقطاع الخدمات عن الأفراد / الجهات المستفيدة في الجهة.

12- التبويب المقترح وفق الخطة الزمنية*

13- قائمة المراجع والمصادر المبدئية:

- 1 https://www.aleqt.com/2017/10/19/article_1269641.html
- 2 <https://aawsat.com/home/article/3159881/%D8%A7%D9%84%D8%AA%D8%B9%D9%84%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9-%D9%82%D8%B5%D8%A9-%D8%A8%D8%AF%D8%A3%D8%AA-%D8%A8%D8%A7%D9%84%D8%AA%D8%AE%D8%B7%D9%8A%D8%B7-%D9%88%D9%86%D8%B6%D8%AC%D8%AA-%D8%A8%D8%B9%D8%AF-%D8%A7%D9%84%D8%AC%D8%A7%D8%A6%D8%AD%D8%A9>
- 3 <https://www.proquest.com/openview/32e4419ca48584e9994c4de8565bc7b3/1?pq-origsite=gscholar&cbl=2044553>
- 4 <https://al-fanarmedia.org/2015/12/arab-universities-are-vulnerable-to-cyber-attacks-experts-say/>
- 5 <https://risk.ksu.edu.sa/node/1239>
- 6 تجربة التعليم الإلكتروني لقسم دراسات المعلومات بجامعة السلطان قابوس في ظل جائحة كورونا
- 7 <https://www.qscience.com/content/journals/10.5339/jist.2022.3?crawler=true>
- 8 <https://www.researchgate.net/publication/345757531> Risks Faces the Universities of Kingdom of Saudi Arabia in Mobile Learning Article *in* Creativity and Innovation Management

Alton, L.; "Employees: Your Strongest or Weakest Link in Cybersecurity," *D!gitalist*, 1 April 2019, -9

<https://www.digitalistmag.com/future-of-work/2019/04/01/employees-your-strongest-or-weakest-link-in-cybersecurity-06197394/>

The Changing Face of Education: Risk, Security and Process Around Distance Learning -10

<https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/the-changing-face-of-education>

[Cybersecurity Awareness Level: The Case of Saudi Arabia University Students - ProQuest](#) -11