مركز أ . د . احمد المنشاوى
للنشر العلمى والتميز البحثى
مجلة كلية التربية
=======

دور الأمن السيبراني في مواجهة المخاطر الإلكترونية لدى أعضاء هيئة التدريس بكلية التربية - جامعة أسيوط

إعـــــــــــــداد

أ.د/ محمد مصطفى محمد حمد
أستاذ أصول التربية ووكيل الكلية
لشئون خدمة المجتمع وتنمية البيئة السابق
كلية التربية- جامعة اسيوط
hamd4572eg@edu.aun.edu.eg

أ.د/ صلاح عبد الله محمد حسن
أستاذ أصول التربية
كلية التربية- جامعة اسيوط
salah.hassan@edu.aun.edu.eg

أ/ أسماء محمد حسن محمد
معيدة بقسم أصول التربية
كلية التربية- جامعة اسيوط
asmaa@aun.edu.eg

﴿المجلد الواحد والأربعون– العدد التاسع – جزء ثاني - سبتمبر ٢٠٢٥ م﴾
http://www.aun.edu.eg/faculty_education/arabic

مستخلص البحث:

هدف البحث إلى التعرف على واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط، وتقديم إجراءات مقترحة لتعزيزه في مواجهة المخاطر الإلكترونية، ولتحقيق ذلك اعتمد البحث على المنهج الوصفي التحليلي، كما استخدمت أداة الاستبانة، وتكون مجتمع البحث من أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط، أما عينة البحث فقد تمثلت في عينة عشوائية بسيطة بلغ عددها(٥١) عضوا، وتوصل البحث للعديد من النتائج من أهمها: أن واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية – جامعة أسيوط جاء بدرجة تحقق متوسطة، حيث تراوح المتوسط الحسابي العام لأبعاد البحث بين (١.٥٠٩٨) و (٢.٠٠٧٨)، بمتوسط عام للاستبانة بلغ (١.٧٨٥٨)، حيث جاء بعد امتلاك الممارسات والسلوكيات في المرتبة الأولى بين أبعاد الأمن السيبراني بمتوسط حسابي (٢.٠٠٧٨)، يليه في المرتبة الثانية امتلاك المهارات التقنية بمتوسط (١.٨٩٠٢)، ثم امتلاك المعرفة والوعي في المرتبة الثالثة بمتوسط (١.٧٠٩٦)، وجاء بعد امتلاك مهارات التعلم المستمر في المرتبة الأخيرة بمتوسط (١.٥٠٩٨)، وبناء على هذه النتائج اقترح البحث عددا من الإجراءات لتعزيز ثقافة الأمن السيبراني كأداة حيوية وفعالة في مواجهة المخاطر والهجمات السيبرانية لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط.

الكلمات المفتاحية: الأمن السيبراني؛ المخاطر الالكترونية؛ أعضاء هيئة التدريس؛ جامعة أسيوط.

The Role of Cybersecurity in Confronting Electronic Risks Among Faculty Members at the Faculty of Education, Assiut University

Mohamed Mostafa Mohamed Mostafa

Department of Foundations of Education

Faculty of Education – Assiut University

hamd4572eg@edu.aun.edu.eg

Salah Abd Allah Mohamed Hassan

Department of Foundations of Education

Faculty of Education- Assiut University

salah.hassan@edu.aun.edu.eg

Asmaa Mohammed Hassan Mohammed

Department of Foundations of Education

Faculty of Education - Assiut University

asmaa@aun.edu.eg

Abstract:

The research aimed to identify the reality of cybersecurity among faculty members at the Faculty of Education - Assiut University, and to present proposed measures to encounter electronic risks. To achieve this, the research relied on the descriptive analytical approach, and a questionnaire tool was used. The research community consisted of faculty members at the Faculty of Education - Assiut University. The research sample was a simple random sample of (51) members. The research reached many results, the most important of which are: The reality of cybersecurity among faculty members at the Faculty of

Education - Assiut University came at a medium level of verification, as the general arithmetic mean of the study dimensions ranged between (1,5098) and (2,0078), with a general average for the questionnaire amounting to (1,7858), where the possession of practices and behaviors came in first place among the dimensions of cybersecurity with an arithmetic mean of (2,0078), followed in second place by the possession of technical skills with an average of (1,8902), then the possession of knowledge and awareness in third place with an average of (1,7096), and the possession of continuous learning skills came in last place with an average of (1,5098). Based on these results, the study proposed a number of measures to enhance the culture of cybersecurity as a vital and effective tool in confronting cyber risks and attacks among faculty members at the Faculty of Education, Assiut University.

Keywords: Cybersecurity; Electronic Risks; Faculty members; Assiut university.

مقدمة البحث:

يشهد العصر الحالي تحولًا رقميًا غير مسبوق يُعد بمثابة قفزة نوعية في عالم التكنولوجيا، حيث أحدث ثورة معلوماتية شاملة امتد تأثيرها إلى مختلف المجالات: العلمية، والتربوية، والاقتصادية، والسياسية، ومع هذا التطور المتسارع والانفجار الهائل في البيانات، أصبح من الصعب مجاراة سرعة انتشار التقنية والسيطرة على تداعياتها؛ مما يستلزم رفع مستويات الجاهزية لمواجهة التحديات والتي على رأسها الجرائم السيبرانية.

ومع التوسع العالمي المتزايد في الاعتماد على تكنولوجيا المعلومات والاتصالات، ارتفعت وتيرة التهديدات التي تستهدف الفضاء السيبراني، حيث أصبح هذا الفضاء ساحة مفتوحة للانتهاكات من قِبل جهات متعددة- سواء كانت دولًا أو مجموعات تمتلك قدرات تقنية متقدمة- ونتيجة لذلك بدأ الاهتمام يتزايد بشكل كبير بمجال الأمن السيبراني، حيث أصبح يُنظر إليه كعنصر أساسي من عناصر الأمن القومي للدول؛ لما له من دور حاسم في حماية البنية التحتية الرقمية والمعلوماتية(عبد الجواد، ٢٠٢٠، ٣٧٠).

ومع كون الأمن ركيزة أساسية لا يمكن تصور تحقيق النمو أو الاستقرار لأي نشاط بدونه، فقد أصبح مع بروز مجتمع المعلومات والفضاء السيبراني أحد أهم قطاعات الخدمات الحديثة التي تُشكّل قيمة مضافة ودعامة حيوية لأنشطة الحكومات والأفراد على حد سواء.

ومع تصاعد الثورة المعلوماتية، ودخول العالم في العصر الرقمي، والتوسع المتسارع في استخدام شبكة المعلومات والإنترنت، وما تحويه من بيانات غاية في الأهمية، أصبح أمن الفضاء السيبراني قضية مركزية تتجاوز حدود الدول، وتتطلب تعاونًا دوليًا لضمان الحماية، حيث ترتّب على ذلك تصاعد الأعباء المالية والإدارية والأمنية التي تتحمّلها الدول في سبيل تحقيق الأمن الرقمي؛ بهدف حماية الأفراد والمجتمعات من التهديدات المتزايدة في هذا الفضاء المفتوح (إحليحل، ٢٠٢٤، ٤٩-٥٠؛ المحيميد، ٢٠٢٣، ٨٥)، ومن هنا ظهر الأمن السيبراني (Cyber Security) كأحد الأبعاد الجديدة في أجندة الدراسات الأمنية، حيث بات يُمثل استجابة استراتيجية للتحديات الناشئة عن توسّع الفضاء الرقمي واعتماده المتزايد في شتى مجالات الحياة.

ومن هنا جاء هذا البحث للكشف عن مدى توفر بعض جوانب ومهارات الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط في مواجهة هذه المخاطر الإلكترونية.

مشكلة البحث:

لاحظت الباحثة أنه في ظل التقدم التكنولوجي المتسارع والاعتماد المتزايد على الفضاء الرقمي، أصبحت الأنظمة والمعلومات عرضة لمجموعة متنامية من المخاطر والتهديدات الإلكترونية: كالهجمات السيبرانية، والاختراقات، وسرقة البيانات، والتلاعب بالمعلومات، حيث تشكل هذه التهديدات تحديا حقيقيا لأمن الأفراد والمؤسسات، ومع ازدياد تعقيد هذه الهجمات وتطور أدواتها تبرز الحاجة الملحة إلى تطوير مهارات الأمن السيبراني للوقاية من هذه المخاطر.

وأكد على ذلك نتائج بعض الدراسات مثل دراسة البعاج(٢٠٢٣)، والتي أكدت على أن الوعي بمفاهيم وتطبيقات الأمن السيبراني جاء بدرجات متوسطة لأفراد العينة، وهو ما يشير الى محدودية وعدم كفاية الوعي بالمفهوم والتطبيقات، بالإضافة لدراسة كل من عبد الجواد وآخرون(٢٠٢٤)، و Khan& Muntaha(2024)، اللذان أظهرا أن برامج التدريب تعزز بشكل كبير قدرة المشاركين على التعرف على محاولات التصيد الاحتيالي، كما أنه يعزز سلوكًا أكثر حذرًا عند التفاعل مع محتوى مشبوه، وانطلاقا من دراسة النقودي(٢٠٢٤)، التي تنص على أن تعزيز الأمن السيبراني يعد عاملاً حاسما في تقليل مخاطر الاختراق والتلاعب، ويدعم استمرارية الأعمال من خلال حماية الأنظمة من الهجمات الالكترونية، تتبلور مشكلة البحث في التساؤل الرئيس التالي:

ما الإجراءات المقترحة لتعزيز ثقافة الأمن السيبراني كأداة حيوية وفعالة في مواجهة المخاطر والهجمات السيبرانية لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط؟

ويتفرع من السؤال الرئيس الأسئلة الفرعية التالية:

١- ما الإطار المفهومي للأمن السيبراني؟
٢- ما الإطار النظري للمخاطر الإلكترونية؟
٣- ما واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط؟
٤- ما الإجراءات المقترحة لتعزيز الأمن السيبراني لدى أعضاء هيئة التدريس في مواجهة المخاطر الإلكترونية؟

٥- أهداف البحث:

١- تعرف الإطار المفهومي للأمن السيبراني.
٢- تعرف الإطار النظري للمخاطر الإلكترونية.
٣- تعرف واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط.
٤- وضع إجراءات مقترحة لتعزيز الأمن السيبراني لدى أعضاء هيئة التدريس في مواجهة المخاطر الإلكترونية؟

أهمية البحث:

أهمية نظرية:

تتمثل في التزويد بإطار نظري عن الأمن السيبراني، بالإضافة إلى تسليط الضوء على بعض المخاطر الإلكترونية.

أهمية تطبيقية:

تتمثل في وضع إجراءات مقترحة لتعزيز الأمن السيبراني لدى أعضاء هيئة التدريس في مواجهة المخاطر الإلكترونية.

مصطلحات البحث:

الأمن السيبراني:

مجموعة من الوسائل التقنية التي تحقق أمن المعلومات الإلكترونية وأمن الحاسبات، والأنظمة الإدارية والبرامج والشبكات، لذا هو أوسع وأشمل من مفهوم أمن المعلومات الإلكترونية، إذ يعد أمن المعلومات الإلكترونية جزءا من الأمن السيبراني(المحيميد، ٢٠٢٣، ٨٥).

مجموع الأطر والهياكل التنظيمية وإجراءات سير العمل، بالإضافة للوسائل التقنية والتكنولوجية التي تهدف إلى حماية الفضاء السيبراني، مع التركيز على ضمان توافر أنظمة المعلومات، وتمتين الخصوصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني(إحليحل، ٢٠٢٤، ٤٨).

وتعرفه الباحثة إجرائيا بأنه: مستوى امتلاك عضو هيئة التدريس للمعارف والمهارات والسلوكيات اللازمة لحماية الأنظمة الإلكترونية، والأجهزة، والمعلومات الشخصية والأكاديمية من التهديدات السيبرانية المحتملة بما في ذلك محاولات الاختراق والهجمات الخبيثة والتصيد الاحتيالي، وسوء استخدام البيانات.

المخاطر الإلكترونية:

الأنشطة الإجرامية التي يتم تنفيذها بواسطة جهاز كمبيوتر أو تقنية حديثة بشكل مباشر أو غير مباشر لارتكاب عمل إجرامي محدد سلفا، سواء كان الهدف أفرادا أو مؤسسات، أو ممتلكات عامة أو خاصة (الضمور، ٢٠٢٤، ٢٥).

مزيج من احتمالية وقوع الحادثة داخل شبكات نظم المعلومات وآثار هذا الحدث على أصول المؤسسة وسمعتها وتؤثر في كل مجالات المؤسسة (بانقاء، ٢٠١٩، ١٢).

وتعرفها الباحثة إجرائيا بأنها: المخاطر والتهديدات التي قد تؤدي إلى خسائر أو أضرار ناجمة عن استخدام التكنولوجيا الرقمية أو الشبكات الإلكترونية، وتشمل هذه المخاطر خطر التعرض لهجمات إلكترونية مثل القرصنة الفيروسات، البرمجيات الخبيثة، فقدان البيانات، أو اختراق الخصوصية، مما يؤثر على سرية البيانات، سلامتها.

حدود البحث:

حد الموضوع : اقتصر البحث على مجال الأمن السيبراني في مواجهة المخاطر الإلكترونية لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط.

الحد البشري: شمل البحث عينة ممثلة من أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط.

الحد المكاني: طبقت الباحثة أداتها على عينة ممثلة في كلية التربية- جامعة أسيوط.

الحد الزماني : فترة تطبيق الأداة .

الإطار النظري:

أولا: الأمن السيبراني

مفهوم الأمن السيبراني:

مصطلح السيبراني مشتق من السايبر (Cyber)، أي مرتبط بثقافة الحاسب ونظم المعلومات، وهو فرع من فروع التكنولوجيا يتمثل دوره في حماية الأنظمة والشبكات والبرامج

من الهجمات الرقمية التي تهدف إلى الوصول للمعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين، وهو ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات ضد هجمات القرصنة بمختلف أنواعها(إحليحل، ٢٠٢٤، ٥٢)، فالأمن السيبراني أساس لأي تحول رقمي، ويعتمد على الاستفادة من التكنولوجيات الرقمية دون خوف، وزيادة فرص الابتكار والتطوير، كما يعد سلاحًا استراتيجيا يمثل نهجا للتخطيط والتصميم والتشغيل، ويتضمن جميع الجوانب التعليمية، والاجتماعية والاقتصادية، والإنسانية(الفنتوخ، ٢٠٢٤، ٤٩).

ويمكننا أن نخلص إلى تعريف الأمن السيبراني بكونه مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، مع تعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني.

ومن خلال ما سبق نجد أن للأمن السيبراني ثلاثة جوانب هي:

- حماية بيانات الأشخاص الإلكترونية.
- حماية مؤسسات الدولة وبياناتها وعملائها.
- حماية الأمن القومى وسلامة المواطنين ورفاهيتهم وخصوصيتهم؛ لكيلا تستخدم هذه البيانات بطرق غير شرعية أو ضد أصحابها. (اليحيائي؛ وعدنان، ٢٠٢٤، ٢١٤-٢١٣)

أهمية الأمن السيبراني:

انطلاقا من كون البيانات والمعلومات والمعارف من الأصول الأساسية، أصبح السعي للمحافظة عليها أمر مهم خاصة مع ظهور الفضاء السيبراني الذي ارتبط بنوع جديد من أنواع الأمن وهو الأمن السيبراني الذي تظهر أهميته فيما يلي:

- يساعد في مكافحة الجريمة السيبرانية وزيادة الوعي العام بها(الشايع، ٢٠١٩، ٥٩).
- يلعب أهمية كبيرة في حماية الأنظمة والشبكات من عمليات الاختراق المختلفة التي تستهدف سرقة المعلومات والسيطرة عليها.
- يساهم في السيطرة على الهجمات الرقمية التي يقودها البعض بهدف سرقة المعلومات والبيانات وإخضاع المستخدمين للابتزاز والمساومة مقابل الحصول على المال.
- أصبح ضروري لحياة الافراد وحماية مصالحهم والحفاظ على صحتهم (إحليحل، ٢٠٢٤، ٥٩).

- المحافظة على أمن المجتمع واستقراره.
- حماية شبكات المعلومات بصورة علمية وتقنية محكمة.
- تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق الدخول إليها (السمحان، ٢٠٢٠، ١١).

مما سبق نرى أن أهمية الأمن السيبراني تبرز في كونه الدرع الواقي للأنظمة الرقمية والمعلوماتية في مواجهة التهديدات المتزايدة والمتطورة، ففي ظل الاعتماد المتنامي على الإنترنت والتكنولوجيا في أداء المهام اليومية والمعاملات الرسمية أصبح تأمين البيانات والمعلومات الحساسة ضرورة حتمية وليس مجرد خيار، فالأمن السيبراني يسهم في الحفاظ على سرية المعلومات، وضمان سلامة العمليات، ومنع الاختراقات التي قد تؤدي إلى خسائر مالية أو تضر بسمعة المؤسسات، بالإضافة للحد من الجرائم الإلكترونية والتجسس الرقمي، فهو يُعزز الثقة في البيئة الرقمية، ويشجع على الاستثمار في التقنيات الحديثة دون خوف من التهديدات السيبرانية.

ثانيا: المخاطر الإلكترونية:

مع زيادة هيمنة تكنولوجيا المعلومات والاتصالات والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة، ظهرت بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير؛ إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الخاصة بحماية المعلومات، والتعرض للهجمات من خلال الفضاء السيبراني(عبد الجواد، ٢٠٢٠، ٣٧٠).

وصلت تهديدات الأمن السيبراني إلى مستويات غير مسبوقة وامتدت آثارها على نطاق واسع، مما يمثل مصدر قلق ملح للأفراد والمؤسسات والحكومات، مع حدوث عواقب محتملة كالخسائر المالية، والإضرار بالسمعة، واختراق المعلومات الشخصية.

خصائص وسمات الجرائم الإلكترونية:

تعرف الجرائم التكنولوجية بأنها الممارسات التي تقع ضد فرد أو مجموعة، مع توفر باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمدًا، أو إلحاق الضرر النفسي والبدني به، سواء أكان ذلك بأسلوب مباشر أم غير مباشر، بالاستعانة بشبكات الاتصال الحديثة كالإنترنت وما تتبعها من أدوات.

وتنقسم الجرائم الإلكترونية لأقسام عديدة منها: جرائم إلكترونية ضد الأفراد: وهي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير مشروعة، وانتحال شخصياتهم، وأخذ الملفات والصور المهمة من أجهزتهم؛ بهدف تهديدهم بها ليمتثلوا لأوامرهم، ومنها جرائم إلكترونية ضد الحكومات، وهي جرائم تهاجم المواقع الرسمية للحكومات وأنظمة شبكاتها لتدميرها، ويسمى الأشخاص المرتكبون لهذه الجريمة بالقراصنة، ومنها جرائم إلكترونية ضد الملكية، وهي جرائم تستهدف المؤسسات الشخصية والحكومية والخاصة؛ لإتلاف الوثائق المهمة أو البرامج الخاصة، كذلك جرائم التشهير، بهدف تشويه سمعة الأفراد، وجرائم السب والشتم والقدح، وجرائم المطاردة الإلكترونية، وهي الجرائم المتعلقة بتعقب أو مطاردة الأفراد عن طريق الوسائل الإلكترونية(الطوخي، ٢٠٢١، ٨٧-٨٨).

ويمكن ذكر بعض السمات والخصائص المرتبطة بالجرائم السيبرانية كما يلي:

١- تتم في بيئة رقمية معلوماتية قوامها النظم المعلوماتية، وأجهزة ومعدات وأدوات وتجهيزات الحاسب الآلي

٢- **ذات طابع خفي**: إن القدرة التقنية التي يتمتع بها المجرم تكون في الغالب أكبر من قدرة الضحية، وقد يكون السبب في ذلك أن الضحايا غالبا ما يخشون الإبلاغ عن الجرائم التي يتعرضون لها، لخوفهم من تأثير ذلك على سمعتهم الشخصية أو المهنية

٣- السرعة في تنفيذها وارتكابها، فهي لا تأخذ وقتا طويلا وتحضيرا مسبقا قبل التنفيذ

٤- ترتكب عن بعد، فالجاني قد يكون في بلد معين والضحية في بلد آخر، دون أن يعرفان بعضهما البعض

٥- عابرة للحدود فهي جرائم غير مدركة للحدود الجغرافية للبلدان، حيث يستطيع الفرد ارتكاب الجرائم السيبرانية من أي مكان في العالم

٦- صعبة الإثبات، حيث إن هذا النوع من الجرائم لا يترك آثارا واضحة ولا ترى بالعين المجردة، فهي تحتاج إلى خبراء وفنيين

٧- جرائم ناعمة لا تتصف بطابع العنف ولا تتطلب القوة العضلية أو البدنية في ارتكابها، لهذا نجد أن المجرم السيبراني يتميز بمهارة وذكاء كبير، ومعرفة بالأساليب التقنية التي يتطلبها لخرق الحواجز الأمنية التقنية

٨- **جرائم فنية تقنية**: عادة ما يكون مرتكبوها خبراء في مجال تكنولوجيا المعلومات، وذو طبيعة وإمكانات خاصة علمية معلوماتية(الضمور، ٢٠٢٤، ٣٢-٣٤).

يتبيّن من التحليل السابق أن الجرائم السيبرانية تختلف بشكل جوهري عن الجرائم التقليدية من حيث طبيعتها، وأساليب تنفيذها، ومدى تأثيرها، بالإضافة إلى نوعية الضحايا المستهدفين بها، كما أن مرتكبي هذا النوع من الجرائم غالبًا ما يكونون من المحترفين ذوي الكفاءة العالية في استخدام التقنيات الحديثة، ويتميزون بقدرتهم على إخفاء هوياتهم الرقمية، فضلًا عن امتلاكهم القدرة على تكرار محاولاتهم الإجرامية باستخدام أساليب متطورة ومتغيرة باستمرار.

صور المخاطر الإلكترونية:

أصبحت المخاطر الإلكترونية من أبرز التحديات التي تواجه الأفراد والمؤسسات في العصر الرقمي، والتي لم تعد تقتصر على مجرد عمليات اختراق، بل تنوعت صورها وأشكالها لتشمل مجموعة واسعة من التهديدات التي تتطور باستمرار مع تطور التكنولوجيا، وتلحق الضرر بالأنظمة والمعلومات، ونذكر منها:

١- الفيروسات والبرامج الخبيثة التي تنتشر عبر الأقراص المرنة المصابة أو مرفقات البريد الإلكتروني

٢- **برامج الفدية والابتزاز:** وهي نوع من البرمجيات الخبيثة التي تُشفّر بيانات الضحية، مما يجعلها غير قابلة للوصول حتى يتم دفع فدية للمهاجم

٣- **التهديدات السحابية**: مع الانتشار الواسع للحوسبة السحابية، ظهرت تهديدات جديدة للأمن السيبراني تتمثل في اختراق حسابات التخزين السحابي، استغلال ثغرات في البنية التحتية السحابية، سرقة بيانات حساسة من التطبيقات السحابية (Dave, et al.,2023, 3-4) .

٤- **الاختراقات السيبرانية**: كاختراق المواقع والصفحات السيبرانية على الإنترنت وتدميرها، أو إلغائها، أو إتلافها، أو التعديل والعبث بالبيانات والمعلومات المتوفرة عليها.

٥- **التجسس السيبراني:** والذي يعد من أخطر الجرائم السيبرانية، فهي نتاج ما أسفر عنه التقدم العلمي والتكنولوجي في شأن أجهزة التصنت الحديثة ذات القدرة الفائقة والدقة البالغة في أعمال التجسس بهدف جمع المعلومات المهمة، أو تعطيل عمل الشبكات العنكبوتية وحواسيبها.

٦- **الإرهاب السيبراني**: وهو استخدام شبكات المعلومات والكمبيوتر من أجل التخويف والإرغام(عبد الجواد، ٢٠٢٠، ٤٠٨-٤١٩).

٧- **سرقة الهوية:** وتتمثل في حصول المهاجم على معلومات شخصية تخص الضحية، كأرقام الهوية أو الحسابات البنكية أو بيانات البطاقات الائتمانية، وتُستخدم هذه المعلومات في أنشطة احتيالية مثل الوصول غير المشروع إلى الحسابات، أو تُباع في الأسواق السوداء عبر الإنترنت، مما يعرّض الأفراد لخسائر مادية وتهديدات أمنية

٨- **الاحتيال المالي عبر بطاقات الدفع:** يُستهدف هذا النوع من الجرائم بيانات بطاقات الائتمان والخصم، ويتم الحصول عليها عبر اختراق قواعد بيانات أو شبكات بيع بالتجزئة.

٩- **قرصنة البرمجيات**: وتشير إلى عمليات النسخ أو التوزيع أو الاستخدام غير المشروع للبرمجيات دون الحصول على ترخيص من مالكيها، هذا النوع من الجرائم لا يُعد فقط انتهاكًا لحقوق الملكية الفكرية، بل يرتبط أحيانًا بانتشار برامج خبيثة تُضمّن في النسخ المقرصنة بهدف الإضرار بالمستخدم أو سرقة بياناته (Abo-Torkhoma, et al. 2023)

استنادا لما سبق يمكن القول بأن تنوع صور المخاطر الإلكترونية وتطورها المستمر يعكس حجم التحديات التي يفرضها الواقع الرقمي المعاصر، ويؤكد على ضرورة تعزيز الوعي الأمني لدى الأفراد والمؤسسات، فالتصدي لهذه المخاطر لا يقتصر على الجانب التقني فقط، بل يتطلب تكاتفا شاملا من الجميع لضمان استخدام آمن للتكنولوجيا في مختلف مجالات الحياة.

الإجراءات المنهجية للبحث:

منهج البحث: في ضوء طبيعة البحث وأهدافه وتساؤلاته استخدم البحث المنهج الوصفي التحليلي.

مجتمع وعينة البحث: تكون مجتمع البحث من أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط ، أما عينة البحث فقد تمثل في عينة عشوائية بسيطة بلغ عددها (٥١) عضو.

أداة البحث: في ضوء طبيعة البحث وأهدافه وتساؤلاته استخدمت الباحثة الاستبانة كأداةً لجمع البيانات؛ والتي تكونت في صورتها النهائية من أربعة أبعاد لقياس واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط كما يلي:

- **البعد الأول:** امتلاك المعرفة والوعي بالأمن السيبراني، ويتضمن(٧) فقرات.
- **البعد الثاني:** امتلاك الممارسات والسلوكيات، ويتضمن(٥) فقرات.
- **البعد الثالث:** امتلاك المهارات التقنية، ويتضمن(٥) فقرات.
- **البعد الرابع:** امتلاك مهارات التعلم المستمر، ويتضمن(٤) فقرات.

تم استخدام مقياس ليكرت الثلاثي للحصول على استجابات أفراد عينة البحث، وذلك وفق درجات الموافقة التالية: نعم، إلى حد ما، لا، ومن ثم التعبير عن هذا المقياس كميًا بإعطاء كل عبارة من العبارات السابقة درجة وفقًا للتالي: نعم (٣) درجات، إلى حد ما (٢) درجتان، لا (١) درجة واحدة.

تحليل بيانات البحث ومناقشة نتائجه:

قامت الباحثة بتحليل ومناقشة النتائج المتعلقة بتساؤلات الاستبيان، وذلك على النحو التالي:

واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط:

جدول رقم (١)

استجابات أفراد العينة لأبعاد واقع الأمن السيبراني بكلية التربية- جامعة أسيوط

الأبعاد	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى التحقق
البعد الأول: امتلاك المعرفة والوعي بالأمن السيبراني	1.7096	.53911	٣	متوسط
البعد الثاني: امتلاك الممارسات والسلوكيات	2.0078	.54840	١	متوسط
البعد الثالث: امتلاك المهارات التقنية	1.8902	.49689	٢	متوسط
البعد الرابع: امتلاك مهارات التعلم المستمر	1.5098	.56560	٤	منخفض
المتوسط العام للاستبانة	1.7858	.43077	-	متوسط

من خلال استعراض النتائج الموضحة بالجدول (١) يتبين أن متوسطات أبعاد واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط تراوحت بين(٢.٠٠٧٨) كحد أقصى للبعد الثاني، و(١.٥٠٩٨) كحد أدنى للبعد الرابع، كما يتضح أن المتوسطات تعكس قيما متوسطة لواقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط، وقد جاء بعد **امتلاك الممارسات والسلوكيات** في المرتبة الأولى في ترتيب أبعاد واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط بمتوسط حسابي(2.0078) وانحراف معياري(.54840)، بينما جاء بعد **امتلاك مهارات التعلم المستمر** في المرتبة الأخيرة في ترتيب أبعاد واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط بمتوسط حسابي(1.5098)، وانحراف معياري(.56560)، وبصفة عامة للاستبانة ككل جاءت بمتوسط حسابي(1.7858)، وانحراف معياري(.43077)، مما يشير إلى أن واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط جاء بمستوى تحقق متوسط.

وفيما يلي تفصيل لاستجابات أفراد العينة لأبعاد واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية- جامعة أسيوط، كما يأتي:

استجابات أفراد العينة على عبارات البعد الأول: امتلاك المعرفة والوعي بالأمن السيبراني:

للتعرف على واقع امتلاك المعرفة والوعي بالأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية جامعة أسيوط، قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية والرتب لاستجابات مفردات عينة البحث على عبارات هذا البعد، وجاءت النتائج كما يوضحها الجدول التالي:

جدول رقم (٢)

استجابات أفراد عينة البحث على عبارات البعد الأول: امتلاك المعرفة والوعي بالأمن السيبراني.

رقم العبارة	العبارات يمتلك عضو هيئة التدريس المعرفة والوعي بـ	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	الفرق بين الأمن السيبراني وأمن المعلومات	1.6863	.70683	٤
٢	الفرق بين الهجوم السيبراني والاختراق الأمني	1.5882	.75303	٦
٣	أنواع الهجمات(DoS، Man-in-the-Middle، التصيد الاحتيالي، وغيرها)	1.4118	.66862	٧
٤	مفاهيم مثل التشفير، المصادقة الثنائية، الجدران النارية	1.6667	.71181	٥
٥	أنواع البرمجيات الخبيثة (فيروسات، برامج تجسس، فيروسات الفدية)	2.1200	.65900	١
٦	مؤشرات الاختراق في البريد أو الملفات	1.7059	.67213	٣
٧	الإجراء المناسب عند التعرض لهجوم أو محاولة اختراق	1.8039	.66392	٢

رقم العبارة	العبارات يمتلك عضو هيئة التدريس المعرفة والوعي بـ	المتوسط الحسابي	الانحراف المعياري	الترتيب
	المتوسط الحسابي العام للبعد	1.7096	.53911	

يتضح من الجدول رقم (٢) ما يأتي:

(أ)- أن هناك تقاربا في درجة موافقة أفراد عينة البحث على العبارات المتعلقة بامتلاك المعرفة والوعي بالأمن السيبراني، حيث تراوحت متوسطات موافقتهم ما بين(٢.١٢٠٠) كحد أقصى، و(١.٤١١٨) كحد أدنى للعبارات، وهي متوسطات تقع في الفئات(الأولى والثانية) من فئات المقياس المتدرج الثلاثي، والتي تُشير إلى درجات تحقق(متوسطة/ ضعيفة) مما يدل على تقارب وجهات نظر أفراد عينة البحث على واقع امتلاك المعرفة والوعي بالأمن السيبراني.

١- جاءت العبارة رقم (٥) وهي" أنواع البرمجيات الخبيثة (فيروسات، برامج تجسس، فيروسات الفدية) " بالمرتبة الأولى بين العبارات المتعلقة بامتلاك المعرفة والوعي بالأمن السيبراني، بمتوسط حسابي(٢.١٢٠٠ من ٣)، وانحراف معياري (65900.).

٢- جاءت العبارة رقم (٣) وهي" أنواع الهجمات(DoS، Man-in-the-Middle، التصيد الاحتيالي، وغيرها "بالمرتبة الأخيرة بين العبارات المتعلقة بامتلاك المعرفة والوعي بالأمن السيبراني، بمتوسط حسابي(١.٤١١٨ من ٣)، وانحراف معياري (66862.).

(ب)– بلغ المتوسط الحسابي العام للبعد المتعلق بامتلاك المعرفة والوعي بالأمن السيبراني(١.٧٠٩٦ من ٣)، وهذا المتوسط يقع بالفئة الثانية من المقياس المتدرج الثلاثي والتي تشير إلى درجة تحقق " متوسطة " أي أن أفراد عينة البحث يمتلكون المعرفة والوعي بالأمن السيبراني بدرجة تحقق متوسطة.

استجابات أفراد العينة على عبارات البعد الثاني: امتلاك الممارسات والسلوكيات:

للتعرف على واقع امتلاك ممارسات وسلوكيات الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية جامعة أسيوط، قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية والرتب لاستجابات مفردات عينة البحث على عبارات هذا البعد، وجاءت النتائج كما يوضحها الجدول التالي:

جدول رقم (٣)

استجابات أفراد عينة البحث على عبارات البعد الثاني: امتلاك ممارسات وسلوكيات الأمن السيبراني.

رقم العبارة	العبارات يعمل عضو هيئة التدريس على	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	استخدم كلمة المرور نفسها لحسابات متعددة لسهولة التذكر	2.3333	.79162	١
٢	تثبيت كلمة المرور الخاصة به إلا في حال حدوث اختراق أو فقدان الوصول	2.2157	.70182	٢
٣	الاحتفاظ بكلمة المرور الخاصة بالبريد الجامعي مكتوبة في مكان يسهل الوصول إليه لتسهيل استخدامها	2.1961	.82510	٣
٤	مشاركة بيانات الدخول إلى منصات التعليم الإلكتروني مع الزملاء أو الطلاب عند الحاجة	1.7059	.80732	٤
٥	تخصيص وقتًا دوريًا لمراجعة إعدادات الأمان في أجهزتهم	1.5882	.72599	٥
	المتوسط الحسابي العام للبعد	2.0078	.54840	

يتضح من الجدول رقم (٣) ما يأتي:

(أ)- أن هناك تقارب في درجة موافقة مفردات عينة البحث على العبارات المتعلقة بامتلاك ممارسات وسلوكيات الأمن السيبراني، حيث تراوحت متوسطات موافقتهم ما بين (٢.٣٣٣٣) كحد أقصى، و(١.٥٨٨٢) كحد أدنى للعبارات، وهي متوسطات تقع في الفئات(الأولى والثانية) من فئات المقياس المتدرج الثلاثي، والتي تُشير إلى درجات تحقق(متوسطة/ ضعيفة) مما يدل على تقارب وجهات نظر أفراد عينة البحث على واقع امتلاك ممارسات وسلوكيات الأمن السيبراني.

١- جاءت العبارة رقم (١) وهي" استخدم كلمة المرور نفسها لحسابات متعددة لسهولة التذكر" بالمرتبة الأولى بين العبارات المتعلقة بامتلاك ممارسات وسلوكيات الأمن السيبراني، بمتوسط حسابي(٢.٣٣٣٣ من ٣)، وانحراف معياري (79162.).

٢- جاءت العبارة رقم (٥) وهي" تخصيص وقتًا دوريًا لمراجعة إعدادات الأمان في أجهزتهم" بالمرتبة الأخيرة بين العبارات المتعلقة بامتلاك ممارسات وسلوكيات الأمن السيبراني، بمتوسط حسابي(١.٥٨٨٢ من ٣)، وانحراف معياري (72599.).

(ب) – بلغ المتوسط الحسابي العام للبعد المتعلق بامتلاك ممارسات وسلوكيات الأمن السيبراني(٢.٠٠٧٨ من ٣)، وهذا المتوسط يقع بالفئة الثانية من المقياس المتدرج الثلاثي والتي تشير إلى درجة تحقق " متوسطة " أي أن أفراد عينة البحث يمتلكون ممارسات وسلوكيات الأمن السيبراني بدرجة تحقق متوسطة.

استجابات أفراد العينة على عبارات البعد الثالث: امتلاك المهارات التقنية:

للتعرف على واقع امتلاك المهارات التقنية للأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية جامعة أسيوط، قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية والرتب لاستجابات مفردات عينة البحث على عبارات هذا البعد، وجاءت النتائج كما يوضحها الجدول التالي:

جدول رقم (٤)

استجابات أفراد عينة البحث على عبارات البعد الثالث: امتلاك المهارات التقنية للأمن السيبراني.

رقم العبارة	العبارات يمتلك عضو هيئة التدريس القدرة على	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	استخدام أدوات فحص الفيروسات وتحليل التهديدات بشكل منتظم	1.7647	.68083	٤
٢	تحديث أنظمة التشغيل والبرامج فور توفر التحديثات الأمنية	2.1176	.62119	١
٣	استخدام كلمات مرور قوية ومتنوعة لكل منصة إلكترونية	2.0196	.70683	٢
٤	استخدام المصادقة الثنائية (2FA) للحسابات الرسمية والشخصية	1.8431	.73137	٣

رقم العبارة	العبارات يمتلك عضو هيئة التدريس القدرة على	المتوسط الحسابي	الانحراف المعياري	الترتيب
٥	تحديد إذا ما كانت شبكة الإنترنت مؤمّنة قبل الاتصال بها	1.7059	.72922	٥
المتوسط الحسابي العام للبعد		1.8902	.49689	

يتضح من الجدول رقم (٤) ما يأتي:

(أ)- أن هناك تجانس في درجة موافقة مفردات عينة البحث على العبارات المتعلقة بامتلاك المهارات التقنية للأمن السيبراني، حيث تراوحت متوسطات موافقتهم ما بين (٢.١١٧٦) كحد أقصى، و(١.٧٠٥٩) كحد أدنى للعبارات، وهي متوسطات تقع في الفئة الثانية من فئات المقياس المتدرج الثلاثي، والتي تُشير إلى درجات تحقق(متوسطة) مما يدل على تجانس وجهات نظر أفراد عينة البحث على واقع امتلاك المهارات التقنية للأمن السيبراني.

١- جاءت العبارة رقم (٢) وهي" تحديث أنظمة التشغيل والبرامج فور توفر التحديثات الأمنية" بالمرتبة الأولى بين العبارات المتعلقة بامتلاك المهارات التقنية للأمن السيبراني، بمتوسط حسابي(٢.١١٧٦ من ٣)، وانحراف معياري (62119.).

٢- جاءت العبارة رقم (٥) وهي" تحديد إذا ما كانت شبكة الإنترنت مؤمّنة قبل الاتصال بها" بالمرتبة الأخيرة بين العبارات المتعلقة بامتلاك المهارات التقنية للأمن السيبراني، بمتوسط حسابي(١.٧٠٥٩ من ٣)، وانحراف معياري (72922.).

(ب) – بلغ المتوسط الحسابي العام للبعد المتعلق بامتلاك المهارات التقنية للأمن السيبراني(١.٨٩٠٢من ٣)، وهذا المتوسط يقع بالفئة الثانية من المقياس المتدرج الثلاثي والتي تشير إلى درجة تحقق " متوسطة " أي أن أفراد عينة البحث يمتلكون المهارات التقنية للأمن السيبراني بدرجة تحقق متوسطة.

استجابات أفراد العينة على عبارات البعد الرابع: امتلاك مهارات التعلم المستمر:

للتعرف على واقع امتلاك مهارات التعلم المستمر للأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية جامعة أسيوط، قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية والرتب لاستجابات مفردات عينة البحث على عبارات هذا البعد، وجاءت النتائج كما يوضحها الجدول التالي:

جدول رقم (5)

استجابات أفراد عينة البحث على عبارات البعد الرابع: امتلاك مهارات التعلم المستمر للأمن السيبراني.

رقم العبارة	العبارات يحرص عضو هيئة التدريس على	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	متابعة دورات تدريبية في الأمن السيبراني بشكل دوري	1.4510	.64230	٤
٢	قراءة تقارير دورية عن أحدث التهديدات السيبرانية عالميًا	1.4902	.64413	٣
٣	تشجيع الزملاء والطلاب على حضور برامج التوعية بالأمن السيبراني	1.5686	.70014	١
٤	المشاركة في خطط الطوارئ أو استراتيجيات الاستجابة التي تعتمدها الجامعة	1.5294	.70294	٢
	المتوسط الحسابي العام للبعد	1.5098	.56560	

يتضح من الجدول رقم (٥) ما يأتي:

(أ)- أن هناك تجانس في درجة موافقة مفردات عينة البحث على العبارات المتعلقة بامتلاك مهارات التعلم المستمر للأمن السيبراني، حيث تراوحت متوسطات موافقتهم ما بين (١.٥٦٨٦) كحد أقصى، و(١.٤٥١٠) كحد أدنى للعبارات، وهي متوسطات تقع في الفئة الأولى من فئات المقياس المتدرج الثلاثي، والتي تُشير إلى درجات تحقق(منخفضة) مما يدل على تجانس وجهات نظر أفراد عينة البحث على واقع امتلاك مهارات التعلم المستمر للأمن السيبراني.

١- جاءت العبارة رقم (٣) وهي" تشجيع الزملاء والطلاب على حضور برامج التوعية بالأمن السيبراني" بالمرتبة الأولى بين العبارات المتعلقة بامتلاك مهارات التعلم المستمر للأمن السيبراني، بمتوسط حسابي(١.٥٦٨٦ من ٣)، وانحراف معياري (70014.).

٢- جاءت العبارة رقم (١) وهي" متابعة دورات تدريبية في الأمن السيبراني بشكل دوري" بالمرتبة الأخيرة بين العبارات المتعلقة بامتلاك مهارات التعلم المستمر للأمن السيبراني، بمتوسط حسابي(١.٤٥١٠ من ٣)، وانحراف معياري (64230.).

(ب) – بلغ المتوسط الحسابي العام للبعد المتعلق بامتلاك مهارات التعلم المستمر للأمن السيبراني(١.٥٠٩٨من ٣)، وهذا المتوسط يقع بالفئة الأولى من المقياس المتدرج الثلاثي والتي تشير إلى درجة تحقق " منخفضة " أي أن أفراد عينة البحث يمتلكون مهارات التعلم المستمر للأمن السيبراني بدرجة تحقق منخفضة.

خلاصة النتائج:

- أظهرت نتائج البحث أن واقع الأمن السيبراني لدى أعضاء هيئة التدريس بكلية التربية – جامعة أسيوط جاء بدرجة تحقق متوسطة، حيث تراوح المتوسط الحسابي العام لأبعاد البحث بين(٢.٠٠٧٨) كحد أقصى للأبعاد، و(١.٥٠٩٨) كحد أدنى، وبمتوسط عام للاستبانة بلغ (١.٧٨٥٨).
- امتلاك الممارسات والسلوكيات جاء في المرتبة الأولى بين أبعاد الأمن السيبراني بمتوسط حسابي (٢.٠٠٧٨)، مما يدل على أن أعضاء هيئة التدريس لديهم مستوى مقبول من الممارسات الوقائية، كاستخدام كلمات مرور قوية ومراجعة إعدادات الأمان.
- امتلاك المهارات التقنية جاء في المرتبة الثانية بمتوسط (١.٨٩٠٢)، مما يشير إلى وجود معرفة متوسطة بالتقنيات الأساسية مثل تحديث الأنظمة والتأكد من أمان الشبكات.
- امتلاك المعرفة والوعي جاء في المرتبة الثالثة بمتوسط (١.٧٠٩٦)، وهو ما يعكس درجة تحقق متوسطة في إدراك مفاهيم مثل أنواع البرمجيات الخبيثة، وأساليب الهجوم السيبراني.
- امتلاك مهارات التعلم المستمر جاء في المرتبة الأخيرة بمتوسط (١.٥٠٩٨)، مما يعكس ضعف الاهتمام بمتابعة التطورات الحديثة في مجال الأمن السيبراني، مثل حضور الدورات أو تشجيع الآخرين على التوعية.

توصيات الدراسة:

لتعزيز الأمن السيبراني لدى أعضاء هيئة التدريس، تقترح الدراسة القيام بالآتي:

١. تنظيم ورش عمل دورية حول المفاهيم الأساسية والمتقدمة للأمن السيبراني.
٢. عقد دورات إلزامية ضمن برامج التطوير المهني لأعضاء هيئة التدريس حول استخدام برامج الحماية.
٣. توفير مطويات إلكترونية أو مكتوبة توضح ممارسات الاستخدام الآمن للإنترنت.
٤. مكافأة المبادرات الفردية في التوعية أو الحماية من مخاطر الفضاء الإلكتروني.
٥. تشجيع ثقافة التعلم المستمر في مجال الأمن السيبراني، من خلال تحفيز حضور الدورات وورش العمل، ومتابعة المستجدات التقنية المرتبطة بحماية البيانات والمعلومات.
٦. تفعيل آليات التقييم الذاتي والدوري للممارسات الأمنية الرقمية مثل إدارة كلمات المرور، واستخدام الشبكات الآمنة، والتعامل مع البرمجيات المجهولة.

قائمة المراجع

أولاً: مراجع عربية:

إحليحل، كريم(٢٠٢٤)، "الأمن السيبراني"، **المجلة الإلكترونية الدولية لنشر الأبحاث القانونية**، المصطفى الغشام الشعيبي، ٤(١٨)، ٤-٧٤.

بانقاء، علم الدين(٢٠١٩)، "مخاطر الهجمات الالكترونية وآثارها الاقتصادية دراسة حالة دول مجلس التعاون الخليجي"، **سلسلة دراسات تنموية**، المعهد العربي للتخطيط بالكويت، (٦٣)، ٧-٦٥.

البعاج، هديل تومان محمد(٢٠٢٣)، "الوعي الاجتماعي بالأمن السيبراني لدى الطلبة (دراسة ميدانية على طلبة الجامعات طلبة كلية الامام الكاظم انموذجا)"، **المؤتمر العلمي السابع تحت شعار العلوم الإنسانية بين التحديات الراهنة والافاق المستقبلية بتاريخ ٢٠٢٣/٧/١**، كلية الآداب- جامعة واسط، ٤٥١-٤٧١.

السمحان، منى عبد الله صالح(٢٠٢٠)، "متطلبات تحقيق الأمن السيراني الأنظمة المعلومات الإدارية جامعة الملك سعود"، **مجلة كلية التربية بالمنصورة**، جامعة المنصورة- كلية التربية، (١١١)، ج١، ٢-٢٩.

الشايع، خالد(٢٠١٩)، **الأمن السيبراني: مفهومه وخصائصه وسياساته**، القاهرة، الدار العالمية للنشر والتوزيع.

الضمور، عدنان محمد(٢٠٢٤)، "الجرائم السيبرانية وأثرها على الأمن المجتمعي بدولة الإمارات العربية المتحدة"، **الفكر الشرطي**، القيادة العامة لشرطة الشارقة - مركز بحوث الشرطة، ٣٣(١٣١)، ١٩-٦٤.

الطوخي، محمد محمد السيد(٢٠٢١)، "تقنيات الذكاء الاصطناعي والمخاطر التكنولوجية"، **الفكر الشرطي**، القيادة العامة لشرطة الشارقة - مركز بحوث الشرطة، ٣٠(١١٦)، ٥٩-١٠٠.

عبد الجواد، أميرة عبد العظيم محمد(٢٠٢٠)، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة البحوث الفقهية والقانونية**، جامعة الأزهر- كلية الشريعة والقانون بدمنهور، (٣٥)، ج٣، ١-١٧٩.

عبد الجواد، سيد نوح سيد؛ وابو الهدى، حسام الدين حسين؛ واسماعيل، الغريب زاهر؛ ومحمود، أيمن جبر(٢٠٢٤)، "تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم"، **مجلة جامعة القيوم للعلوم التربوية والنفسية**، ١٨(٩)، ٣١٧-٣٦٨.

الفنتوخ، عبد الله بن عبد الرحمن(٢٠٢٤)، "المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم"، **مجلة الجامعة الإسلامية للعلوم التربوية والاجتماعية**، الجامعة الإسلامية بالمدينة المنورة، (١٨)، ٤٧- ٩٤.

المحيميد، باسم بن إبراهيم(٢٠٢٣)، "دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية"، **مجلة العلوم التربوية**، جامعة الأمير سطام بن عبدالعزيز، ٩(٤)، ٨٣-١١٦.

النقودي، سوزي فاروق(٢٠٢٤)، "أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية"، **مجلة البحوث المحاسبية**، ١١(٤)، ١٧٠-٢١٦.

اليحيائي، نوال بنت عيسى محمد؛ وعدنان، محمد عزرين بن محمد(٢٠٢٤)، "أهمية الأمن السيبراني في العملية التعليمية والقيم الدينية"، **مجلة مجمع**، جامعة المدينة العالمية، (٤٨)، ٢٠١-٢٣٨.

ثانياً: مراجع أجنبية:

Abd AL-latif, H., & Ali, G. S(2023), Cybercrime Types and Digital Forensic Tools , **Alandalus Universtity For Science & Technology**,*11*(19).

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D.(2023), The new frontier of cybersecurity: emerging threats and innovations. **In 2023 29th International Conference on Telecommunications (ICT)**, IEEE, 1-6.

Khan, M. H., & Tul Muntaha, S(2024).Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study, **World Journal of Advanced Research and Reviews**, 23(2), 1663-1673.