ISSN : 2543-3938 - EISSN : 2602-7771

الوعي بالأمن السيبراني في الممارسة التعليمية في ظل التحول الرقمي بجامعة الجزائر 3
دراسة مسحية على عينة من أساتذة كلية علوم الاعلام والاتصال -نوفمبر 2025-

Cybersecurity awareness in Teaching practices in the context of Digital Transformation at The University of Algiers 3: A Survey study of a sample of professors from the faculty of information and communication, sciences -November 2025-

حياة ابراهيمي

[1] جامعة الجزائر 3 (الجزائر) Brahimi.hayat@univ-alger3.dz

مخبر استخدام وتلقي المنتجات الإعلامية والثقافية في الجزائر

تاريخ الإستلام: 2026/04/03 تاريخ القبول: 2026/05/23

ملخص الدراسة:

في ظل التحول الرقمي والحديث عن توجه الجامعة الجزائرية إلى جامعات الجيل الرابع، أصبح الحديث عن حماية البيانات الرقمية من الضروريات التي تستوجب رفع أعلى درجات الوعي لمواجهة مختلف التهديدات السيبرانية، خاصة في ظل تطور التقنيات المستعملة في اختراق البيانات الرقمية وتنفيذ الهجمات السيبرانية.

وهدفنا من خلال دراستنا إلى معرفة درجة الوعي بالأمن السيبراني لدى أساتذة كلية علوم الإعلام والاتصال بجامعة الجزائر 3، وذلك من خلال معرفة اتجاهاتهم وحجم معارفهم فيما يخص حماية البيانات الرقمية أثناء استخدامهم لمختلف المنصات الرقمية، وخلصت الدراسة إلى ضرورة تبني استراتيجية تسمح بتكوين الأساتذة في المجال الرقمي من خلال برمجة دورات تكوينية باشراك مختصين في المجال، والحرص على خلق بيئة رقمية آمنة وفعالة.

الكلمات المفتاحية: الأمن السيبراني; الوعي الرقمي; جامعة الجيل الرابع.

***

Abstract:

In the context of digital transformation and the strategic orientation of the University of Algiers 3 toward becoming a fourth-generation university, the issue of digital data protection has emerged as a fundamental necessity. It calls for elevating awareness to the highest levels in order to مواجهة diverse cyber threats, particularly in light of the rapid evolution of technologies used for breaching digital data and conducting cyberattacks.

The present study aims to assess the level of cybersecurity awareness among faculty members at the Faculty of Information and Communication Sciences at the University of Algiers 3. This is achieved by examining their attitudes and the extent of their knowledge regarding the protection of digital data during their use of various digital platforms. The study concludes with the need to adopt a strategic framework that supports the development of faculty competencies in the digital domain, through the organization of structured training programs in collaboration with field specialists, while emphasizing the importance of fostering a secure and efficient digital environment

Keywords: Cyber Security; Digital Awareness; Fourth-Generation University.

I. مقدمة

يعيش العالم اليوم ثورات رقمية كبيرة اجتاحت مختلف القطاعات، أين أصبح الاعتماد على الرقمنة والوسائط المتعددة والذكاء الاصطناعي ضرورة حتمية. فموضوع تخزين البيانات والمعلومات بالاعتماد على تكنولوجيا عالية الدقة والتعقيد يحيلنا إلى الحديث عن توفر آليات لحماية المعلومات الرقمية ومواجهة مختلف المخاطر المتعلقة بانتهاك البيانات وتسريبها.

فيعد موضوع الأمن السيبراني من أهم المواضيع التي تسعى الحكومات إلى احتواءها، من خلال إصدار القوانين واللوائح التشريعية التي تهدف إلى حمايات البيانات الرقمية.

تسعى وزارة التعليم العالي في الجزائر إلى تبني التحول الرقمي وتحويل مؤسساتها الجامعية إلى جامعات من الجيل الرابع، ومن بينها جامعة الجزائر 3 التي عملت على اعتماد المعايير الدولية للجامعات من الجيل الرابع مع نهاية 2025. وهو ما يعني رقمنة الخدمات واستحداث منصات رقمية ذات طابع بيداغوجي وخدماتي وبحثي. فمن أجل ضمان تحول رقمي آمن وجب العمل على مواجهة الثغرات الأمنية والتهديدات السيبرانية،

وذلك ما يدعو لزيادة الوعي بالأمن السيبراني لدى مختلف الفاعلين، خاصة في ظل تطور التقنيات يوميا ما يتطلب جهود مضاعفة. ويعد الأساتذة طرفا مهما في استراتيجية تعزيز الأمن السيبراني في الوسط الجامعي، وعليه فنتجه من خلال دراستنا إلى طرح الإشكالية التالية:

ما مستوى الوعي بالأمن السيبراني لدى أساتذة كلية علوم الإعلام والاتصال بجامعة الجزائر 3؟ وكيف يتجلى أثناء ممارستهم التعليمية الرقمية؟

II. الإطار المنهجي:

أ. تساؤلات الدراسة:

1. ما هو مفهوم الأمن السيبراني ومكوناته لدى عينة الدراسة؟
2. كيف يواجه المبحوثين المخاطر الرقمية أثناء استخدامهم المنصات التعليمية ومختلف الموارد الرقمية؟
3. هل يلتزم المبحوثون بإجراءات الأمان والحماية الرقمية في تعاملهم مع البيانات الرقمية؟
4. هل تعمل جامعة الجزائر 3 على تعزيز وتنمية الوعي بالأمن السيبراني لدى أساتذتها؟

ب. أهداف الدراسة:

نسعى من خلال هذه الدراسة إلى معرفة مستوى وعي الأساتذة الجامعيين بكلية علوم الإعلام والاتصال بجامعة الجزائر 3 بالأمن السيبراني، وما مدى انعكاس هذا على ممارستهم التعليمية في ظل التحول إلى جامعة الجيل الرابع، وذلك من خلال معرفة مفهوم الوعي السيبراني لدى عينة الدراسة والذي يتضمن المخاطر الرقمية وتعاملهم معها. بالإضافة إلى تقييم دور جامعة الجزائر 3 في نشر الوعي السيبراني وسط أساتذة الجامعة حسب عينة الدراسة.

ت. أهمية الدراسة:

تبرز أهمية الدراسة من أهمية الموضوع الذي يعد إضافة معرفية مهمة لجامعة الجزائر3 في تبنيها للتحول الرقمي، فمعرفة واقع الوعي بالأمن السيبراني لدى الأساتذة يساهم في تحليل الواقع، كما أن نتائج الدراسة

تساهم في اعداد استراتيجية لنشر ثقافة الأمن السيبراني وتحديد نقاط الضعف التي يمكن تحسينها من خلال تبني ورشات تكوينية موجهة لكافة الفاعلين في جامعة الجزائر 3 خاصة هيئة التدريس.

ث. منهج وأدوات الدراسة:

يمثل المنهج أساس أي بحث علمي، كونه يعبر عن الخطوات العلمية التي يسلكها الباحث بغية الوصول إلى نتائج دقيقة وقابلة للتعميم. فحسب "موريس أنجرس" فهو الإجابة المقدمة للسؤال كيف نصل إلى الأهداف، في حين أن التقنيات هي الوسيلة المتبعة بغية الوصول لهذه الأهداف (أنجرس، 2006).

وحسب دراستنا فقد تم الاستعانة بالمنهج المسحي، الذي يهتم بجمع البيانات وتحليلها مما يسمح بوصف الواقع، ويستخدم هذا المنهج بكثرة في تخصص علوم الإعلام والاتصال. ويعمل المنهج المسحي على دراسة مختلف القضايا على طبيعتها دون تزييف، ويساعد على اكتشاف العلاقة بين الظواهر عن طريق جمع معلومات كاملة تمكننا من إيجاد حل منطقي ومعقول للقضية محل الدراسة والبحث (بوحوش، د.ت).

ج. أدوات الدراسة:

تعتمد دراستنا على أداة الاستبيان الالكتروني، الذي يعد أداة لجمع البيانات والذي يرسل المبحوثين من خلالها أجوبتهم عبر شبكة الأنترنيت من خلال الولوج إلى رابط معين يمكنهم من الإجابة عن الأسئلة، وقدم تم تصميم الاستبيان بالاعتماد على google Forms.

وتتضمن الاستمارة 19 سؤال مقسمة على المحاور التالية:

1. مفهوم الأمن السيبراني حسب عينة الدراسة.
2. مواجهة المخاطر الرقمية أثناء استخدام المبحوثين للمنصات التعليمية ومختلف الموارد الرقمية.
3. التزام المبحوثون بإجراءات الأمان والحماية الرقمية في تعاملهم مع البيانات الرقمية.
4. دور جامعة الجزائر 3 في تعزيز وتنمية الوعي بالأمن السيبراني حسب عينة الدراسة.

ح. مجتمع الدراسة والعينة:

يعرف مجتمع البحث بأنه جميع المفردات ذات العلاقة بمجتمع البحث (مرسلي، 2013)، فتحديده من أهم المراحل المنهجية التي تتطلب الدقة مما يمكننا من التوصل إلى نتائج دقيقة وشاملة. فبعد تعيين مفردات البحث وخصائصها ومدى تجانسها اتجهنا إلى تحديد عينة الدراسة، من خلال اختيار عدد من أفراد المجتمع الاحصائي المراد دراسته فتعد العينة حسب موريس أنجرس أنها مجموعة فرعية من عناصر مجتمع البحث (انجرس، 2004) ، ويتم اختياراها وفق ضوابط علمية من أجل تحصيل معلومات دقيقة يمكن لاحقا تعميمها على كل مفردات المجتمع الكلي للبحث. وفي دراستنا حول الوعي السيبراني في الممارسة التعليمية للأساتذة الجامعيين في ضوء التحول الرقمي بجامعة الجزائر 3 تم اللجوء إلى العينة القصدية والتي هي عينة غير احتمالية، يختار فيها الباحث مفردات بحثه بشكل حر حسب ما يراه يتماشى مع أهداف دراسته.

ويختار الباحث في العينة القصدية عدد قليلا من المفردات التي تملك صفة التمثيل المطلوبة، ولا يلجأ إلى استعمالها إلا إذا اضطرته ظروف البحث في اختيار عدد قليل جدا من المفردات (بدوي، 1978).

وتشمل عينتنا أساتذة كلية علوم الإعلام والاتصال لأنهم الأكثر ارتباطا بموضوع البحث. فقد بلغ عدد المجتمع الكلي للدراسة 252 أستاذا، وقد وزعت الاستمارة على18.6% منهم أي ما يعادل 47 استمارة خضعت للتحليل الاحصائي.

III. مفاهيم الدراسة:

1. الأمن السيبراني:

لغة: يمكن أن نجزأ هذا المصطلح إلى لفظين: "الأمن" و "السيبراني".

الأمن: من منة، يأمنه، أمنا: وثق به واطمأن إليه.

السيـــبراني: كلمة cyber لفظة يونانية الأصل مشتقة من كلمة kybernetes أي الشخص الذي دير السفينة، وقد نسب بعض الدارسين الكلمة إلى عالم الرياضيات الأمريكي Norbert wieners(1964_1894تعبيرا عن التحكم الآلي (OERCOMMONS، بلا تاريخ).

اصطلاحيا: قدمت العديد من التعاريف لمفهوم الأمن السيبراني، فحسب تعريف وزارة الدفاع الأمريكي pintagon فهي كل الإجراءات التنظيمية التي تسعى لحماية المعلومات بمختلف أشكالها، الكترونية كانت أم مادية، من الجرائم التي تسعى إلى مهاجمتها وتخريبها أو التطفل عليها. كما أنه "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات" (برغوث، 2003).

كما يعني العملية التي نقوم فيها بالتركيز على نقل المعلومات الرقمية وتخزينها ومعالجتها باستخدام بشكل آمن، والاهتمام بمختلف أساليب الدفاع والحماية على كل أنظمة الحواسيب والشبكات الذكية. وذلك بتشفير البيانات وتحديث الأنظمة ومواجهة الفيروسات وبرامج التهكير.

إجرائيا: نقصد بالأمن السيبراني في دراستنا مجموعة المعارف التي يمتلكها الأساتذة الجامعيين حول إجراءات حماية المعلومات والبيانات الرقمية أثناء استخدامهم لمختلف المنصات الرقمية أثناء ممارستهم التعليمية، وقدرتهم على التصدي لمختلف التهديدات والاختراقات السيبرانية.

2. الوعي الرقمي:

يعرف بأنه القدرة على استعمال مختلف الأجهزة الرقمية والحصول من خلالها على المعلومات الرقمية، بالإضافة إلى القدرة على التفكير التحليلي وفهم طرق استخدام الوسائط والمعلومات.

وحسب منظمة اليونيسكو (2013) فقد حددت الوعي الرقمي بأنه امتلاك الأفراد لمجموعة من المهارات والقدرات في عملية البحث عن المعلومات الالكترونية واسترجاعها وتقييمها وتطبيقها مع الآخرين (غربي و مسعودي، 2024).

إجرائيا: نقصد بالوعي الرقمي في دراستنا مختلف المؤهلات والمعارف الضرورية التي يجب أن يملكها أساتذة جامعة الجزائر 3، والتي تمكنهم من استخدام الأجهزة الرقمية والاستفادة من قواعد البيانات في العملية التعليمية مثل منصة بروغرس ومودل. من خلال القدرة على جمع المعلومات وتنظيمها واستخدامها بكفاءة.

3. جامعة الجيل الرابع:

هي الجامعة التي تعتمد على ريادة الأعمال والابداع والابتكار مع تبني نهج كاملا متعدد التخصصات يعمل على تطوير الأبحاث العلمية التي تخدم حاجيات المجتمع، مستعينة بالتكنولوجيا الحديثة وتقنيات الذكاء الاصطناعي (بعلي و حمو، 2025).

وتتمثل أبعاد جامعات الجيل الرابع في مجموعة من النقاط والتي تسهم في اخراج الجامعة من اطارها الكلاسيكي وهي (الخير، 2025):

- ✓ تتميز عملية التدريس بالإبداع والابتكار، مع توظيف التكنولوجيا وتحقيق ما يسمى بالتعلم الذكي.
- ✓ عالمية البحث العلمي من خلال ربط التعاون ما بين الجامعات واعتماد مشاريع بحثية مشتركة تعمل على خدمة المجتمعات المحلية، والمساهمة في اعداد القادة مع تحقيق نمو اقتصادي مستدام.
- ✓ التحول الرقمي في الوظيفة الإدارية وتكييف الهيكل التنظيمي مع هذا التوجه، مع ضرورة تعميم استخدام التكنولوجيا وتطوير البنى التحتية والاستعانة بتقنيات تكنولوجية متطورة.
- ✓ الريادة واغتنام الفرص والابداع في حل مشكلات المجتمع.

إجرائيا: هي اعتماد جامعة الجزائر 3 على تحول يرتكز على دمج التكنولوجيات الحديثة في المنظومة التعليمية، مع التفاعل المباشر مع المحيط الاقتصادي والاجتماعي والاعتماد على تبني ريادة الأعمال والابتكار كركائز أساسية في البرامج البحثية والأكاديمية.

IV. الجانب التطبيقي:

1) المحور الأول: البيانات الشخصية للمبحوثين

الجدول 1 يمثل توزيع العينة حسب متغير السن

الفئة العمرية	التكرار	النسبة المئوية%
أقل من 30 سنة	1	%2.1
من 30 إلى 40 سنة	18	%38.3
من 41 إلى 50 سنة	18	%38.3
أكثر من 50 سنة	10	%21.3
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

نلاحظ من خلال الجدول رقم 1 أن الفئة العمرية الأكثر مشاركة تنقسم وبالتساوي على الفئتين من 30 إلى 40 سنة ومن 41 إلى 50 سنة على التوالي بنسبة قدرت ب 38.3 % أي ما يعادل 18 مفردة لكل فئة، في حين بلغ عدد المبحوثين من الفئة أكثر من 50 سنة 21.3% أي 10 مبحوثين. أما من يبلغون من العمر أقل من 30 سنة فكانوا ممثلين بمبحوث واحد أي بنسبة 2.1%.

ويفسر هذا التوزيع بكون أغلب المبحوثين يتراوح سنهم ما بين 30 إلى 50 سنة عموما، وهي فئة نشطة مهنيا يمكنها التفاعل إلى حد ما مع موضوع دراستنا.

الجدول رقم 2 يمثل توزيع العينة حسب متغير الخبرة المهنية

الخبرة المهنية	التكرار	النسبة المئوية
أقل من 5سنوات	9	%19
من 6 إلى 10 سنوات	7	%15
أكثر من 10 سنوات	31	%66
المجموع	**47**	**100%**

المصدر: من إعداد الباحثة

نلاحظ من خلال الجدول رقم 2 بأن 66% من المبحوثين تتجاوز خبرتهم المهنية أكثر من 10 سنوات وهو ما يعادل 31 مفردة، في حين بلغت خبرة المبحوثين الذين يحوزون على أقل من 5 سنوات خبرة 19% أي 9 مبحوثين. فيما يبلغ عدد المبحوثين الذين يملكون خبرة مهنية تتراوح بين 6 إلى 10 سنوات 7 مبحوثين أي ما يعادل 15%.

فباعتبار أن المبحوثين ذو الخبرة أكثر من 10 سنوات الأكثر تمثيلا في الدراسة، فهو مؤشر جيد لتقييم مكانة الأمن السيبراني في العملية التعليمية في ظل الاعتماد على التكنولوجيات الحديثة ومختلف المنصات الرقمية في عملية التدريس.

الجدول رقم 3 يمثل توزيع العينة حسب متغير الرتبة المهنية

الرتبة المهنية	التكرار	النسبة المئوية
أستاذ مساعد	8	%17
أستاذ محاضر	23	%49
أستاذ التعليم العالي	16	%34
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

نلاحظ من خلال الجدول رقم 3 بأن 49% من المبحوثين أي ما يعادل 23 مفردة برتبة أستاذ محاضر، في حين بلغ عدد المبحوثين المشاركين برتبة أستاذ التعليم العالي 34% أي 16 مبحوث، في حين بلغ عدد المبحوثين برتبة أستاذ مساعد 8 مبحوثين ما يعادل 17%.

2) **المحور الثاني: مفهوم الأمن السيبراني**

الجدول رقم 4 خاص بمفهوم الأمن السيبراني عند المبحوثين

الاجابات	التكرار	النسبة المئوية
حماية الأجهزة من الفيروسات	15	%32
حماية المعلومات والبيانات من الاختراق	46	%98
مراقبة النشاطات على الانترنيت	10	%10

المصدر: من إعداد الباحثة

بالرجوع إلى معطيات الجدول 4 الخاص بمفهوم الأمن السيبراني لدى عينة الدراسة، نلاحظ بأن 98% من المبحوثين يرون أن مفهوم الأمن السيبراني يتعلق بحماية المعلومات والبيانات من الاختراق، في حين يؤكد 32% من المبحوثين على أن الأمن السيبراني يتضمن أيضا جزء خاص يتعلق بحماية الأجهزة من الفيروسات. فيما أكد 10% من المبحوثين أن مراقبة النشاطات على الانترنيت يدخل ضمن نطاق الأمن السيبراني.

فإجماع المبحوثين على اعتبار الأمن السيبراني يشمل أمن البيانات من الاختراق، يعد نقطة إيجابية ذلك أن حماية البيانات والمعلومات الخاصة من الاختراق والوصول غير المصرح به من أهم النقاط الواجب التركيز عليها في إطار التعامل مع مختلف المنصات الرقمية في العملية التعليمية.

إلا أن مراقبة النشاطات على الانترنيت وحماية الأجهزة من الفيروسات يعدان من المجالات المهمة للأمن السيبراني، بحيث أنه من الضروري العمل على استخدام مختلف البرامج الخاصة بمكافحة الفيروسات والبرامج والهجمات الضارة. والتقييم الدوري لنظام الأمان.

الجدول رقم 5 خاص بالمجالات التي يشملها الأمن السيبراني حسب المبحوثين

الإجابات	التكرار	النسبة المئوية
أمن المعلومات الشخصية	18	%38
أمن الشبكات	16	%34
أمن المؤسسات الاكاديمية	13	%28
المجموع	47	%100

المصدر: من إعداد الباحثة

نلاحظ من خلال البيانات المقدمة في الجدول 5 أن المبحوثين يرون بأن الأمن السيبراني يشمل عدة مجالات، من بينها أمن المعلومات حسب 38% من المبحوثين، في حين أكد 34% بأنه يتعلق بأمن الشبكات. أما 28% فيرون أن أمن المؤسسات الأكاديمية يعتبر ضمن مجالات الأمن السيبراني.

إن فهم المبحوثين لمجالات الأمن السيبراني مهم في عملية بناء الوعي بالأمن السيبراني، فلا يحصر الأمر في مجال حماية الشبكات فقط بل يشمل أمن المعلومات الشخصية وأمن الشبكات والبنى التحتية الرقمية وضمان سلامتها وكذا أمن المؤسسات الأكاديمية وأنظمتها من مختلف الهجومات والتهديدات السيبرانية. إن إدراك المبحوثين لضرورة هذا التكامل بين مختلف المستويات الفردية، التقنية والمؤسساتية يعمل على تشكيل وعي قوي في المجال السيبراني ويضمن التزام المبحوثين بمختلف إجراءات السلامة الرقمية.

الجدول رقم 6 خاص بمتابعة المبحوثين لمستجدات الأمن السيبراني

الاجابات	التكرار	النسبة المئوية
دائما	6	%13
أحيانا	32	%68
نادرا	9	%19
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

من خلال الجدول رقم 6 نلاحظ بأن 68% من المبحوثين هم أحيانا مطلعين على مستجدات الأمن السيبراني، في حين بلغ عدد المبحوثين المتابعين دائما للمستجدات 13%، في حين أكد 19% من عينة البحث بأنهم نادرا ما يتابعون أخبار ومستجدات الأمن السيبراني.

ففي ظل التطور الرقمي والاعتماد على التكنولوجيات الحديثة واستخدام المنصات الرقمية في العملية التعليمية في جامعة الجزائر 3، فإنه من المهم التفكير في أهمية المتابعة الجادة لقضايا الأمن السيبراني. فعدم الاهتمام بهذا المجال قد يعرض بيانات الأساتذة إلى التهديدات الإلكترونية ما يؤثر على أمن بيانات الجامعة وهو ما يؤدي إلى عواقب وخيمة على المؤسسة.

الجدول رقم 7 حول المصادر الاساسية لمعلومات المبحوثين حول الأمن السيبراني

الاجابات	التكرار	النسبة المئوية
الانترنيت ووسائل الاعلام	34	%72
التكوين الأكاديمي	11	24%
الزملاء	2	%4
المجموع	**47**	**100%**

المصدر: من إعداد الباحثة

من خلال الجدول رقم7 يؤكد 72% من المبحوثين بأنهم يستقون معلوماتهم المتعلقة بالأمن السيبراني من الأنترنيت ووسائل الاعلام، في حين يرى 24% يجمعون المعلومات من التكوينات الأكاديمية، و4% يرجعون مصدر معلوماتهم إلى الزملاء.

وعليه فاعتماد نسبة كبيرة من المبحوثين على الأنترنيت ووسائل الاعلام في الاطلاع على المعلومات المتعلقة بالأمن السيبراني يرجع إلى سهولة الوصول إلى المعلومات وتوفرها، إلا أنه من المهم أيضا أن يعتمد المبحوثين على الدورات التكوينية المختصة لما توفره من معلومات دقيقة ومفصلة باستخدام مصطلحات دقيقة تدمج بين النظري والتطبيقي. وهو ما يؤهلهم لاحقا إلى الاستعداد أكثر لحماية أجهزتهم وبياناتهم من مختلف الاختراقات والهجمات الالكترونية.

3) **المحور الثالث:** مواجهة المخاطر الرقمية أثناء استخدام المبحوثين للمنصات التعليمية ومختلف الموارد الرقمية.

الجدول رقم 8 خاص بتعرض المبحوثين لمحاولة الاختراق الالكتروني

الاجابات	التكرار	النسبة المئوية
نعم	22	%47
لا	25	%53
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

حسب الجدول رقم8 فإن 47% من المبحوثين تعرضوا إلى محاولة الاختراق الإلكتروني، في حين لم يتعرض 53% من المبحوثين لذلك. ورغم ذلك فإن نسبة 47% تعد مهمة في تفسير النتائج، ذلك أن عدم تمكن المبحوثين من حماية حساباتهم من الاختراق يمكن أن يعرضهم ويعرض الجامعة إلى تعطيل الأنظمة وتسريب البيانات وتضرر السمعة.

وكانت وزارة التعليم العالي الجزائرية قد نبهت سابقا إلى وجود اختراق وقرصنة للكمبيوتر في حسابات البريد الالكتروني (COMB)، والذي بسببه تم تسريب عدة بيانات، داعية إلى ضرورة القيام بعدة إجراءات لحماية الحسابات مع التأكيد على عدم استخدام البريد الشخصي في المهام المهنية (جريدة البلاد الالكترونية، 2021).

الجدول رقم 9 حول نوع المخاطر الرقمية التي يواجهها المبحوثين

الاجابات	التكرار	النسبة المئوية
اختراق البريد الالكتروني	15	%32
الفيروسات	46	%98
سرقة المعلومات	10	%10
اختراق حساب الفيسبوك	1	%3.3

المصدر: من إعداد الباحثة

يبين الجدول رقم 9 بأن المبحوثين يواجهون عدة مخاطر رقمية، فحسب 98% من المبحوثين فانهم تعرضوا إلى هجومات فيروسية، في حين أكد32% من عينة الدراسة بأن بريدهم الإلكتروني تعرض للاختراق، أما 10% فقد تمت سرقة بياناتهم ومعلوماتهم، في حين أكد 3.3% بأن حساباتهم عبر منصة الفيسبوك قد تعرضت للاختراق.

فتعرض المبحوثين للهجمات الفيروسية يشكل خطرا كبيرا على البيانات من خلال السيطرة على الحواسيب وسرقة البيانات الحساسة والمعلومات المالية وحذف الملفات، بالإضافة إلى إمكانية مراقبة سلوكيات المستخدمين دون علمهم عن طريق برامج التجسس. ومن البرمجيات الخبيثة نجد دودة الحواسيب، حصان طروادة، البوتات والروت كيت.

كما أن تعرض المبحوثين لاختراق البريد الالكتروني يحمل أيضا عدة انعكاسات سلبية على الجامعة، من خلال تسريب البيانات الشخصية للأساتذة، واستخدام حساباتهم لانتحال الهوية. بالإضافة إلى التلاعب بالبيانات الأكاديمية، حذف ملفات بحثية وحتى تعطيل السير البيداغوجي بسبب الهجمات السيبرانية.

الجدول رقم 10 حول الإجراءات التي يتخذها المبحوثين عند مواجهة تهديدات رقمية

الاجابات	التكرار	النسبة المئوية
أتجاهله	11	%24
أستعين بخبير تقني	28	%60
أبلغ الجهات الأمنية	8	%17
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

حسب الجدول رقم10 فقد أكد 60% من المبحوثين أي ما يعادل 28% مبحوثا بأنهم يستعينون بخبير تقني عند مواجهة أي تهديدات رقمية، في حين أكد 24% منهم بأنهم يقومون بتجاهل الأمر، أما 17% من المبحوثين فقد أكدوا بأنهم يفضلون تبليغ الجهات الأمنية.

فمن الجيد أن يستعين المبحوثين بالخبراء التقنيين في مجال الأمن السيبراني لكونهم يملكون خبرات مهمة في تأمين البيانات واسترجاع الحسابات، وتقييم الثغرات وإيجاد حلول دفاعية. ومن جهة أخرى فتجاهل التهديدات الرقمية وعدم التبيغ عنها أو عدم محاولة مواجهتها سيضع البيانات وخاصة ما ارتبط منها بالجامعة أمام خطر كبير. فتبني التحول الرقمي الذي قدم العديد من الإيجابيات، فتح مجالا واسعا أماما التهديدات السيبرانية التي قد تعمل على تعطيل الأنظمة الحيوية والتسبب في عدة خسائر للمؤسسات الحيوية في المجتمع، وهو ما يتطلب تظافر الجهود من أجل بناء استراتيجية دفاعية متكاملة العناصر يعد فيها الأساتذة جزءا مهم لحماية المؤسسة الجامعية.

الجدول رقم 11 خاص بآراء المبحوثين بشأن المخاطر الرقمية كتهديد محتمل للأساتذة الجامعيين

الاجابات	التكرار	النسبة المئوية
نعم	38	%81
لا	9	%19
المجموع	47	%100

المصدر: من إعداد الباحثة

بناء على المعلومات المقدمة في الجدول رقم 11 فقد أكد 38 مبحوثا أي ما يعادل نسبة 81% بأن المخاطر الرقمية تشكل تهديدا للأساتذة الجامعيين، في حين رأى 19% من المبحوثين بأن المخاطر الرقمية لا تشكل أي تهديد للأساتذة الجامعيين.

فإقرار المبحوثين بأن المخاطر المتعلقة باستخدام الوسائط الرقمية في العمل الأكاديمي يشكل تهديدا للأساتذة الجامعيين، يعكس درجة من الوعي بضرورة إيجاد حلول دفاعية تقيهم من تبعيات هذه المخاطر. خاصة في ظل اعتماد جامعة الجزائر 3 وخاصة كلية علوم الإعلام والاتصال على المنصات الرقمية سواء للتدريس كموودل، أو منصة بروغرس أو البوابة الالكترونية التي تعتبر وسيلة رقمية تربط بين الكلية والأساتذة وتسمح بتبادل المعلومات والبيانات.

الجدول رقم 12 خاص بقدرة المبحوثين على حماية بياناتهم الشخصية والمهنية من المخاطر الرقمية

الاجابات	التكرار	النسبة المئوية
قوية	2	%4
متوسطة	30	%68
ضعيفة	15	%32
المجموع	47	%100

المصدر: من إعداد الباحثة

من خلال الجدول رقم 12 فوصف 68% من المبحوثين قدرتهم على حماية بياناتهم الشخصية والمهنية من المخاطر الرقمية بالمتوسطة، في حين أكد 15 مبحوثا أي 32% من عينة الدراسة بأن قدراتهم ضعيفة في حماية بياناتهم. أما 4% من المبحوثين فأقروا بأنهم يملكون قدرات قوية في مجال حماية البيانات الشخصية والمهنية من المخاطر الرقمية.

فالنتائج المقدمة توضح بأن نسبة كبيرة من المبحوثين غير قادرين فعليا على حماية بياناتهم الرقمية، وهو ما يعد تهديدا حقيقيا لأمن البيانات، فعدم امتلاك القدرة القوية على مواجهة التهديدات السيبرانية سيزيد من احتمالية تعرضهم لمحاولات اختراق أو استغلال لبياناتهم الشخصية والمهنية سواء على منصات التواصل الاجتماعي، البريد الالكتروني أو المنصات التعليمية.

المحور الرابع: التزام المبحوثون بإجراءات الأمان والحماية الرقمية في تعاملهم مع البيانات الرقمية.

الجدول رقم 13 حول استخدام المبحوثين لكلمات مرور قوية ومعقدة

الاجابات	التكرار	النسبة المئوية
نعم	30	%64
لا	17	%36
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

نلاحظ من خلال الجدول رقم 13 بأن 64% من المبحوثين يستخدمون كلمات مرور قوية ومعقدة في مختلف حساباتهم على المنصات الرقمية، في حين أكد 36% من عينة الدراسة أن كلمات المرور المستخدمة غير قوية.

فاستعمال كلمات المرور القوية والمعقدة يعمل على التقليل من مخاطر خرق الأمان، فقد أثبتت الدراسات بأن معظم حالات الاختراق بسبب استخدام كلمات مرور بسيطة وسهلة التخمين. فوفقا لتقرير تحقيقات خرق البيانات DBIR لعام 2022 من VERIZONاستخدمت 81% من الانتهاكات المتعلقة بالقرصنة كلمات مرور ضعيفة (opswat، 2023).

الجدول رقم 14 خاص بتغيير كلمة المرور بانتظام

الاجابات	التكرار	النسبة المئوية
نعم	7	%15
لا	13	%28
حسب الحاجة	27	%57
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

حسب الجدول رقم.14 فقد أكد 57% من المبحوثين بأنهم يغيرون كلمة السر حسب الحاجة، في حين لا يقوم بذلك 28 % من المبحوثين. فيما أكد 15% من أفراد العينة بأنهم يقومون بتغيير كلمات المرور المستخدمة في مختلف حساباتهم الرقمية بانتظام.

تعد كلمات المرور من الخطوات المهمة لحماية الحسابات على المنصات الرقمية من الاختراقات والهجومات السيبرانية، وتعتمد قوتها على طولها، عدم استخدام معلومات شخصية، استخدام كلمات مبتكرة ورموز مختلفة.

فانتظار حدوث مشكلة ما من أجل تغيير كلمة المرور يدل على ضعف الوعي الرقمي لدى المبحوثين، ذلك أن المستخدم لا يمكنه دائما الكشف عن الاختراقات الصامتة والتي تسهل تسريب بياناته دون علمه. وعليه من بين إجراءات الأمان التغيير الدوري لكلمات المرور.

الجدول رقم 15 خاص بمشاركة المبحوثين لحساباتهم الشخصية مع الآخرين

الاجابات	التكرار	النسبة المئوية
نعم	16	%34
لا	31	%66
المجموعة	**47**	**%100**

المصدر: من إعداد الباحثة

يشير الجدول رقم 15بأن 66% من عينة الدراسة لا يقومون بمشاركة حساباتهم الشخصية مع الآخرين، في حين يقوم 34 %من المبحوثين بمشاركة حساباتهم الشخصية مع الآخرين.

فعدم مشاركة الحسابات الشخصية عبر الانترنيت -خاصة- يعد ضرورة قصوى من أجل منع مختلف الانتهاكات والاستعمالات غير المشروعة للحسابات ما قد يورط أصحابها. ذلك أن مشاركة الحسابات الشخصية قد يعرض صاحبه إلى إمكانية استغلال معلوماته الشخصية، التعرض للاحتيال المالي أو الابتزاز.

الجدول رقم 16 يتعلق بمدى احتفاظ المبحوثين بنسخ احتياطية عن ملفاتهم الاكاديمية والبحثية

الاجابات	التكرار	النسبة المئوية
نعم	41	%87
لا	6	%13
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

يشير الجدول رقم 16إلى أن 87% من عينة الدراسة يحتفظون بنسخ احتياطية عن ملفاتهم الأكاديمية والبحثية، في حين أن 13% من المبحوثين لا يقومون بذلك.

فالنتائج المقدمة توضح إدراك المبحوثين لأهمية تأمين المعلومات، فالنسخ الاحتياطي للملفات خاصة الأكاديمية والبحثية يعد بديلا في حال تعرض الجهاز أو البريد الالكتروني لأي هجوم سيبراني أو حتى خللا في الأجهزة والبرامج. ومن بين طرق حفظ المعلومات نجد التخزين السحابي مثل icloud، محركات الأقراص الصلبة HDD، محركات أقراص الفلاش USB...الخ.

4. **المحور الخامس: دور الجامعة في تعزيز ثقافة الأمن السيبراني**

الجدول رقم 17 يوضح إجابات المبحوثين حول تنظيم الجامعة لورشات ودورات تكوينية حول الأمن السيبراني

الاجابات	التكرار	النسبة المئوية
نعم	15	%32
لا	17	%36
لا أعلم	15	%32
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

حسب معطيات الجدول رقم 17 فإن جامعة الجزائر 3 لا تنظم ورشات ودورات حول الأمن السيبراني حسب 36% من المبحوثين، في حين أكد 32% من المبحوثين أن الجامعة تنظم دورات وورشات خاصة بالأمن السيبراني. فيما أكد 32% من المبحوثين بجهلهم عما إذا كانت الجامعة تقدم دورات خاصة بالمجال السيبراني.

فبرمجة الدورات التكوينية حول الأمن السيبراني يعمل على ضمان تحول رقمي آمن، ذلك أن زيادة الوعي الرقمي يساهم في بناء استراتيجية أمنية تحمي الجامعة من المخاطر التي تهدد وجودها. فالأمن السيبراني لا يختزل في مصالح الاعلام الآلي بل يجب أن يشمل مختلف الفاعلين في المؤسسة خاصة الأساتذة كونهم يمارسون العملية التعليمية عبر وسائط رقمية.

الجدول رقم 18 خاص بمدى توفر الجامعة على سياسات او تعليمات حول حماية المعلومات

الاجابات	التكرار	النسبة المئوية
نعم	9	%19
لا	18	%38
لا أدرى	20	%43
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

حسب الجدول 18فان 43% من المبحوثين يؤكدون بأن جامعة الجزائر 3 لا يعلمون إن كانت جامعة الجزائر 3 توفر سياسات أو تعليمات حول حماية المعلومات، في حين أكد 38% من المبحوثين بأن الجامعة محل الدراسة لا توفر أي تعليمات متعلقة بحماية المعلومات. أما 19% من المبحوثين أكدوا بأن جامعة الجزائر 3 تحوز على مجموعة من السياسات او التعليمات الخاصة بحماية البيانات والمعلومات.

إن إقرار 43% من المبحوثين بعدم درايتهم بتوفر جامعة الجزائر 3 على تعليمات حول حماية المعلومات يعكس ضعفا في آليات الاتصال الداخلي في المؤسسة، وهو ما يؤدي الى عدم وصول القرارات والتعليمات الإدارية الى جميع الفاعلين.

أما تأكيد38% من المبحوثين عدم وجود التوجيهات الرسمية حول حماية البيانات، يجعل من الأساتذة يعتمدون على مجهوداتهم الفردية في حماية بياناتهم. فمن أجل بناء سلوك رقمي آمن يجب على الجامعة أن تعمل على وضع نصوص تنظيمية واضحة ومفصلة تتعلق بمسؤوليات المستخدمين وأليات التعامل مع الحوادث السيبرانية، في شكل مبسط يوضح كيفية حماية البريد الالكتروني، كلمات المرور وغيرها.

الجدول رقم 19 حول توفير الجامعة للدعم التقني للأساتذة عند مواجهة مشاكل أمنية رقمية

الاجابات	التكرار	النسبة المئوية
نعم	10	%21
لا	37	%79
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

نلاحظ من خلال إجابات المبحوثين المقدمة في الجدول رقم 19 بأنه وحسب 79% منهم فإن جامعة الجزائر 3 لا تقدم أي دعم تقني للأساتذة عند مواجهة مشاكل أمنية رقمية، في حين أكد 21 من المبحوثين أكدوا بأن جامعتهم تقدم مساعدات تقنية لحل مختلف المشاكل الرقمية.

فعدم حرص مسؤولي جامعة الجزائر 3 على مرافقة الأساتذة تقنيا وتقديم الدعم لهم سيؤثر على جودة التدريس والتحول الرقمي، لأن حماية بيانات الأستاذ هي حماية لبيانات المؤسسة ككل.

الجدول رقم 20 خاص بتقييم المبحوثين لاهتمام جامعة الجزائر3 بتعزيز ثقافة الأمن السيبراني

الاجابات	التكرار	النسبة المئوية
كبير	2	%4
متوسط	17	%36
ضعيف	28	%60
الجميع	**47**	**%100**

المصدر: من إعداد الباحثة

يوضح الجدول رقم 20**بأنه** وحسب 60% من عينة الدراسة فإنهم يرون أن اهتمام جامعة الجزائر 3 بتعزيز ثقافة الأمن السيبراني ضعيف، في حين اعتبر 36% من المبحوثين أنهم يصنفون اهتمام الجامعة بمجال الأمن السيبراني بالمتوسط، في حين يرى 4% من المبحوثين أن هناك اهتماما كبيرا من قبل جامعة الجزائر 3 بتعزيز ثقافة الأمن السيبراني.

فعدم اهتمام جامعة الجزائر 3 بتعزيز ثقافة الأمن السيبراني في ظل تبنيها للتحول الرقمي يعد تناقضا كبيرا، ذلك أن أي توسع رقمي غير مرفق بالثقافة الأمنية السيبرانية سيعرض الجامعة الى مخاطر عديدة تهدد بياناتها وتجعلهم عرضة للاختراق أو التسريب.

الجدول رقم 21 يوضح المقترحات التي يقدمها المبحوثين من أجل تعزيز ثقافة الأمن السيبراني في جامعة الجزائر3

الاجابات	التكرار	النسبة المئوية
برمجة دورات تكوينية وتدريبية للأساتذة في مجال الأمن السيبراني	38	%81
توفير شبكة انترنيت قوية ومركزية مدعمة بفريق تقني محترف	4	%8.5
انشاء نظام خاص بالتبليغ عن الانتهاكات والاختراقات بالشراكة مع المؤسسات الأمنية	4	%8.5
ادماج الأمن السيبراني في المقررات الدراسية الاساسية	1	%2
المجموع	**47**	**%100**

المصدر: من إعداد الباحثة

نلاحظ من خلال الجدول رقم 21 اقتراحات المبحوثين من أجل تعزيز ثقافة الأمن السيبراني في جامعة الجزائر3، إذ أكد 81% من المبحوثين أي ما يعادل 38 مفردة بأن الجامعة يجب أن تعمل على برمجة دورات تكوينية وتدريبية في مجال الأمن السيبراني، بالإضافة إلى توفير شبكة انترنيت قوية ومركزية مدعمة بفريق تقني محترف حسب 8.5% من المبحوثين. بالإضافة إلى انشاء نظام خاص بالتبليغ عن الانتهاكات والاختراقات بالشراكة مع المؤسسات الأمنية حسب 8.5% من المبحوثين. في حين يرى 2% من المبحوثين بأنه من الضروري إدماج الأمن السيبراني في المقررات الدراسية الأساسية.

فإجماع نسبة كبيرة من المبحوثين على أهمية التكوين والتدريب في مجال الأمن السيبراني يؤكد ادراكهم لشدة المخاطر الموجودة على شبكة الانترنيت. وعليه فمسؤولي جامعة الجزائر 3 مطالبين ببرمجة مجموعة من الأيام التكوينية من أجل تدريب الموظفين على الوعي بالأمن الالكتروني لتزويدهم بمختلف المهارات لحماية بياناتهم والمعلومات الحساسة من الاختراق أو غيرها من الهجمات الالكترونية، والتي بدورها تحمي البنية التحتية

لتكنولوجيا المعلومات في المؤسسة. ووفقا لدراسة أجرتها Kaspersky فإن الاستخدام غير المناسب لموارد تكنولوجيا المعلومات من قبل الموظفين يشكلان اثنين من أكبر التهديدات التي تواجهها الشركات (kaspersky، بلا تاريخ).

كما أن توفير شبكة أنترنيت قوية يضمن سرعة انتقال المعلومات ويقلل من المشاكل التقنية مما يرفع كفاءة العمل، خاصة في حال تكليف فريق تقني محترف والذي سيساعد في تعزيز مستوى الأمن السيبراني ومراقبة محاولات الاختراق والتحديث المستمر للبرمجيات، مما يقلل من مخاطر اختراق الأنظمة وما يليها من انعكاسات سلبية على البيانات.

ويرى المبحوثين أنه من بين الحلول إنشاء نظام خاص بالتبليغ على الانتهاكات والاختراقات وربطها بأجهزة الأمن، مما يسمح بالمعالجة الفورية للقضايا ذات الصلة بالوسط الجامعي. كما أنه من المهم حسب عينة الدراسة ادراج مقاييس تعنى بالأمن السيبراني لأنها تعد من المداخل الأساسية لرفع مستوى الوعي وتنمية السلوك الرقمي.

III. نتائج الدراسة:

من خلال دراستنا توصلنا إلى ما يلي:

- يجمع المبحوثين أن مفهوم الأمن السيبراني بتعلق بحماية المعلومات والبيانات من الاختراق، في حين يؤكد 32% من المبحوثين على أن الأمن السيبراني يتضمن أيضا جزء خاص يتعلق بحماية الأجهزة من الفيروسات. فيما أكد 10% من المبحوثين أن مراقبة النشاطات على الانترنيت يدخل ضمن نطاق الأمن السيبراني.
- يرى المبحوثين بأن الأمن السيبراني يشمل عدة مجالات، من بينها أمن المعلومات، أمن الشبكات. وبنسبة أقل أمن المؤسسات الأكاديمية يعتبر ضمن مجالات الأمن السيبراني.
- 68% من المبحوثين هم **أحيانا** مطلعين على مستجدات الأمن السيبراني.
- يستقي 72% من المبحوثين معلوماتهم المتعلقة بالأمن السيبراني من الأنترنيت ووسائل الاعلام بدرجة كبيرة،
- 47% من المبحوثين تعرضوا إلى محاولة الاختراق الإلكتروني، من بينهم 98% تعرضوا لهجومات فيروسية ، أما 10% فقد تمت سرقة بياناتهم ومعلوماتهم، في حين أكد 3.3% بأن حساباتهم عبر منصة الفيسبوك قد تعرضت للاختراق.
- أكد 60% من المبحوثين بأنهم يستعينون بخبير تقني عند مواجهة أي تهديدات رقمية.
- أكد 38 مبحوثا أي ما يعادل نسبة 81% بأن المخاطر الرقمية تشكل تهديدا للأساتذة الجامعيين.
- وصف 68% من المبحوثين قدرتهم على حماية بياناتهم الشخصية والمهنية من المخاطر الرقمية بالمتوسطة.
- 64% من المبحوثين يستخدمون كلمات مرور قوية ومعقدة في مختلف حساباتهم على المنصات الرقمية.
- أكد 57% من المبحوثين بأنهم يغيرون كلمة السر حسب الحاجة، فانتظار حدوث مشكلة ما من أجل تغيير كلمة المرور يدل على ضعف الوعي الرقمي لدى المبحوثين.
- 66% من عينة الدراسة لا يقومون بمشاركة حساباتهم الشخصية مع الآخرين، وهو ما يعد ضرورة قصوى من أجل منع مختلف الانتهاكات والاستعمالات غير المشروعة للحسابات ما قد يورط أصحابها.
- إن 87% من عينة الدراسة يحتفظون بنسخ احتياطية عن ملفاتهم الأكاديمية والبحثية.
- جامعة الجزائر 3 لا تنظم ورشات ودورات حول الأمن السيبراني حسب 36% من المبحوثين.
- يؤكد 43% من المبحوثين بأنهم لا يعلمون إن كانت جامعة الجزائر 3 توفر سياسات أو تعليمات حول حماية المعلومات، وهو ما يعكس ضعفا في آليات الاتصال الداخلي في المؤسسة، ما يعني عدم وصول القرارات والتعليمات الإدارية الى جميع الفاعلين.

- تأكيد38% من المبحوثين عدم وجود التوجيهات الرسمية حول حماية البيانات، يجعل من الأساتذة يعتمدون على مجهوداتهم الفردية في حماية بياناتهم.
- حسب 79% منهم فإن جامعة الجزائر 3 لا تقدم أي دعم تقني للأساتذة عند مواجهة مشاكل أمنية رقمية، وهو سيؤثر على جودة التدريس والتحول الرقمي، لأن حماية بيانات الأستاذ هي حماية لبيانات المؤسسة ككل.
- حسب 60% من عينة الدراسة فإنهم يرون أن اهتمام جامعة الجزائر 3 بتعزيز ثقافة الأمن السيبراني ضعيف، يعد تناقضا كبيرا، ذلك أن أي توسع رقمي غير مرفق بالثقافة الأمنية السيبرانية سيعرض الجامعة الى مخاطر عديدة تهدد بياناتها وتجعلهم عرضة للاختراق أو التسريب.
- أكد 81% من المبحوثين بأن الجامعة يجب أن تعمل على برمجة دورات تكوينية وتدريبية في مجال الأمن السيبراني، بالإضافة إلى توفير شبكة انترنيت قوية ومركزية مدعمة بفريق تقني محترف حسب 8.5% من المبحوثين. بالإضافة إلى انشاء نظام خاص بالتبليغ عن الانتهاكات والاختراقات بالشراكة مع المؤسسات الأمنية حسب 8.5% من المبحوثين. في حين يرى 2% من المبحوثين بأنه من الضروري إدماج الأمن السيبراني في المقررات الدراسية الأساسية.
- فإجماع نسبة كبيرة من المبحوثين على أهمية التكوين والتدريب في مجال الأمن السيبراني يؤكد ادراكهم لشدة المخاطر الموجودة على شبكة الانترنيت.

IIII. خاتمــة:

لتحقيق تحول رقمي آمن نحو جامعة من الجيل الرابع، وجب إرساء دعائم قوية للأمن السيبراني باعتباره عنصرا مهما لتوفير الحماية الضرورية للمنظومة الرقمية للجامعة. فالأمن السيبراني لم يعد مجرد خيارا ثانويا بل ركيزة لأي تحول رقمي خاصة في مجال حماية البيانات الأكاديمية والإدارية من مختلف التهديدات المتزايدة في الفضاء الرقمي.

وباعتبار الأستاذ فاعلا أساسيا في إنجاح العملية التعليمية الرقمية ومحورا رئيسيا في حماية البيئة المعلوماتية،وجب الاهتمام بتكوين وعي رقمي فعال من خلال برمجة دورات تكوينية عالية المستوى وتفعيل برامج توعية تواكب التطورات المتسارعة في المجال الرقمي، لان التكوين هو مسار مستدام من أجل بناء ثقافة رقمية آمنة داخل المؤسسات الجامعية تجمع بين الوعي والمسؤولية والممارسة السليمة. ناهيك عن ضرورة انفتاح الجامعة على المحيط الخارجي من خلال تبني شراكات استراتيجية مع الجهات والمؤسسات المختصة في الأمن السيبراني، وهو ما يتيح تطوير آليات الحماية بناء على المعايير العالمية وهو ما يقوي قدرة الجامعة على مواجهة التحديات السيبرانية.

المراجـــــــــع:

الكتب العلمية:

1. أحمد بن مرسلي. (2013). *الأسس العلمية لبحوث الإعلام والاتصال* (الإصدار 1). الجزائر: الورسم للنشر والتوزيع.
2. أحمد زكي بدوي. (1978). *معجم المصطلحات الاجتماعية*. بيروت: مكتبة لبنان.
3. عمار بوحوش. (د.ت). *دليل الباحث في المنهجية وكتابة الرسائل الجامعية* (الإصدار 2). الجزائر: المؤسسة الوطنية للكتاب.
4. موريس انجرس. (2004). *منهجية البحث العلمي في العلوم الإنسانية* (الإصدار 2). (صحراوي بوزيد، و آخرون، المترجمون) الجزائر: دار القصبة للنشر.

المقالات العلمية:

5. ساعد غربي، و كمال مسعودي. (2024). أثر اكتساب الوعي الرقمي في تنمية مهارات استخدام برمجيات إدارة المحتوى الرقمي لدى الأساتذة الجامعيين. *مجلة الحقوق والعلوم الإنسانية، 17*(2)، 25.
6. ليلى بن برغوث. (2003). الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي، التهديدات، التقنيات، التحديات وآليات التصدي. *المجلة الدولية للاتصال الاجتماعي، 10*(1)، 477.
7. مولود بعلي، و بوعلام حمو. (2025). دور الأداء الرقمي في تعزيز تبني نموذج جامعات الجيل الرابع في الجزائر: دراسة تحليلية للتحديات والفرص. *مجلة حقوق الانسان والحريات العامة، 10*(1)، 233.
8. ميلود زيد الخير. (2025). ملامح التحول الرقمي نحو تجسيد جامعة الجيل الرابع. *ملامح التحول الرقمي نحو تجسيد جامعة الجيل الرابع، مجلة إضافات اقتصادية، 9*(2)، 412.

المو اقع الالكترونية:

9. kaspersky. (بلا تاريخ). *ما هو التدريب على الوعي الأمني*. تاريخ الاسترداد 18 جانفي, 2026، من https://me.kaspersky.com: https://me.kaspersky.com/resource-center/definitions/what-is-security-awareness-training
10. OERCOMMONS. (بلا تاريخ). تاريخ الاسترداد 03 04, 2026، من www.oercommons.org: https://oercommons.org/courseware/lesson/94012/student/?section=5
11. opswat. (4 ماي, 2023). تاريخ الاسترداد 10 02, 2026، من www.arabic.opswat.com: https://arabic.opswat.com/blog/2023-world-password-day-6-ways-to-strengthen-password-security
12. جريدة البلاد الالكترونية. (12 03, 2021). *وزارة التعليم العالي تحذر من اختراق وقرصنة للحواسيب عن طريق البريد الالكتروني*. تاريخ الاسترداد 26 جانفي, 2026، من https://www.elbilad.net/national/%D9%88%D8%B2%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%AA%D8%B9%D9%84%D9%8A%D9%85-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%8A-%D8%AA%D8%AD%D8%B0%D8%B1-%D9%85%D9%86-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D9%88%D9%82%D8%B1%D8%B5%D9%86%D8%A9