جامعة الشهيد حمه لخضر-الوادي

كلية العلوم الاجتماعية والانسانية

مخبر التنمية الاجتماعية وخدمة المجتمع

ينظم :

الملتقى الوطني الموسوم ب:الأمن السيبراني ورهانات الأمن الشامل في الجزائر

المحور الرابع : مكونات المجتمع المدني وثقافة الأمن السيبراني (قراءات في الوعي المجتمعي/قراءات في خطاب الكراهية)

عنوان المداخلة: احتياجات أفراد المجتمع للأمن السيبيراني

دراسة على عينة من أساتذة التعليم الثانوي

الاسم	قويدر	عبد اللطيف
اللقب	لخويمس	قنوعة
التخصص	تربية وأنظمة تعليمية	علم النفس التربوي
الرتبة	طالب دكتوراه	أستاذ محاضر أ
المؤسسة	جامعة الشهيد حمة لخضر الوادي	جامعة الشهيد حمة لخضر الوادي
ب الالكتروني	lekhouimes-kouider@univ-eloued.dz	guenoua-abdellatif@univ-eloued.dz

الملخص :

تهدف هذه الدراسة الى معرفة مدى حاجة أساتذة التعليم الثانوي بضرورة الأمن السيبراني، ومعرفة المجالات التي بحاجة للأمن السيبراني من طرفهم، ثم معرفة فيما اذا كان عدم الأمن السيبراني عائقا لهم في استعمال الوسائل الرقمية، حيث استخدمنا المنهج الاستكشافي واخترنا المقابلة كأداة لجمع البيانات وقد أجريت الدراسة على عينة متكونة من 28 أستاذا للتعليم الثانوي من ثانوية ديدي صالح بولاية الوادي في الفترة من 05 مارس2024 الى غاية 05 أبريل 2024، وتوصلت الدراسة الى النتائج التالية: نسبة 89.28 % من أساتذة التعليم الثانوي يحسون بالحاجة الى الأمن السيبراني، ومن أهم المجالات الي يحتاجون فيها للأمن السيبراني البرامج التي تخزن المعلومات الشخصية، مواقع التواصل الاجتماعي، بطاقات التداول الالكترونية و المجال التربوي وقطاع التعليم ونسبة 75% منهم لم يكن عدم الأمن السيبراني عائقا لهم في استعمال المعلوماتية.

الكلمات المفتاحية:

الأمن السيبراني، اساتذة التعليم الثانوي، البرامج الإلكترونية، الرقمة.

Abstract :

This study aims to know the extent to which secondary education teachers need cyber security, and to know the areas that need cyber security on their part, and then to find out whether the lack of cyber security is an obstacle to them in using digital means, as we used the exploratory approach and chose the interview as a tool for collecting data. The study was conducted. On a sample of 28 secondary education teachers from Didi Salah Secondary School in El Oued State in the period from March 2024 to April 5, 2024, the study reached the following results: 89.28% of secondary education teachers feel the need for cyber security, and one of the most important areas in which they need security is Cyber programs that store personal information, social networking sites, electronic trading cards, the educational field and the education sector, and 75% of them did not find the lack of cyber security an obstacle to using information technology.

key words:

Cyber security, secondary education teachers, electronic, digital programs

مقدمة:

إن التطور الكبير والمتسارع للتكنلوجيا الحديثة في القرن الواحد والعشرين والذي شمل كل ميادين الحياة في ظل التحول الرقمي الكبير والذي أسهم في ربح الوقت والجهد وتلبية الحاجيات هو ما جعل المختصين في المجال المعلوماتي الالكتروني (السيبراني) يعتبرون أن هذا المجال هو أحد ميادين النزاعات في هذا العصر بعد الأرض، البحر، الجو والفضاء (بارة،2017).

يعدّ الأمن السيبراني ضروريًا لحماية المعلومات الحساسة للأفراد والدول على حدٍ سواء، وهو ما جعل فضاء القوة السيبراني له الأهمية في الاستراتيجيات العسكرية والمدنية (كلاع،2022) فهو يُشكل خط الدفاع الأول ضدّ التهديدات الإلكترونية المتزايدة في عصرنا الرقمي، وتظهر أهميته من خلال حماية البيانات الشخصية كونه يُحافظ على سرية المعلومات الشخصية والمالية للمستخدمين، ويمنع وصول المُخترقين إليها ممّا يُشكل خطرًا على حياتهم وسلامتهم اضافة لكونه يُقي من سرقة البيانات الحساسة للدول، ممّا قد يُهدد أمنها القومي واستقرارها، كما أنه يدعم النمو الاقتصادي ويُشجع على الاستثمار في الخدمات السحابية، حيثُ يُؤمّن بيئة آمنة لتخزين البيانات تُعزّز ثقة المستخدمين ويُحافظ على استمرارية عمل المؤسسات والشركات، ويُقلّل من خطر تعرّضها لهجمات إلكترونية تُعيق عملياتها وتُلحق بها خسائر فادحة ومن خلاله يتم تعزيز الثقة في العالم الرقمي كونه يُضفي شعوراً بالأمان على مستخدمي الإنترنت، ويُشجّعهم على إجراء المعاملات الإلكترونية بكلّ ثقة ويُحسّن من سمعة الشركات والمؤسسات، ويُعزّز من قدرتها على جذب العملاء وبناء علاقات ثقة معهم. كما أنه يُساهم في الحدّ من الأنشطة غير القانونية على الإنترنت، مثل الاحتيال وسرقة الهوية والابتزاز، وكونه يحمي المستخدمين من المحتوى الضارّ والفيروسات والبرامج الخبيثة التي تُهدّد أجهزتهم وبياناتهم فهو يشكل حماية خصوصية الأفراد مما يُتيح للمستخدمين التحكّم ببياناتهم الشخصية، ويُمنع من جمعها أو استخدامها دون موافقتهم، يُحافظ على حرية التعبير ويُساهم في خلق بيئة رقمية آمنة تُتيح للجميع التعبير عن آرائهم دون خوف. وبرغم ما توصي به الدراسات في هذا المجال حماية من أي هجوم اختراق كأن يجب أن تكون كلمات المرور معقدة وقوية وأن تغيَّر بانتظام ولكل تطبيق كلمة مرور خاصة به والتحيين المنتظم للبرامج عبر إجراء تسييري للتحيينات مخطط ومعروف مسبقا وأن تكون للأفراد استراتيجية حفظ البيانات منتظمة و مخطط لها بشكل صحيح ودقيق وتجنب تثبيت برامج أو تطبيقات من مواقع غير رسمية وغيرها من الاحتياطات الأمنية (بوقرص،2022).

وفي بحثنا هذا نهدف الى معرفة حاجة وإحساس أساتذة التعليم الثانوي بضرورة الأمن السيبراني كونهم أحد شرائح أفراد المجتمع الأكثر وعيا بأهميته، ومعرفة المجالات التي بحاجة للأمن السيبراني من طرفهم، ثم معرفة فيما اذا كان عدم الأمن السيبراني عائقا لهم في استعمال الوسائل الرقمية.

إن "الثورة التقنية والتطور التكنولوجي المتسارع وثورة المعلومات (مجتمع ما بعد المعلومات) وتجليات الفضاء السيبراني حيتم على الدول إعادة صياغة الكثير من المفاهيم كالقوة، الحرب، الصراع، الردع، باتخاذ التدابير التي تسهم في الحد من مخاطر تهديدات الفضاء السيبراني على الأمن القومي العالمي"(مسيكة، 2022، ص.459)، واذ يُعدّ الأمن السيبراني ضرورةً لا غنى عنها في عصرنا الرقمي، ورغم الإيجابيات التي حملتها الانترنت والعالم الرقمي الالكتروني، فقد رافق ذلك العديد من المخاطر والتهديدات بصورة الكترونية طالت الأشخاص والمؤسسات بل هددت الدول في أمنها واستقرارها، وفي الجزائر تشير الإحصائيات الى انتشار واسع لما يعرف بالجريمة الإلكترونية في السنوات الأخيرة في ظل توجه الجزائر نحو مقاربة الحكومة الالكترونية (بارة،2017)." والمخاطر السيبراني المستحدثة التي تمثل خطرا وتهديدا كبيرا على الفرد والمجتمع وكذلك على الأجهزة الأمنية للدولة"(قطاف،،ص.32 ،2022).

وبناء على ما تقدم نطرح التساؤلات التالية : هل يحس أساتذة التعليم الثانوي بالحاجة الى ضرورة الأمن السيبراني؟ وماهي المجالات التي يحتاجون فيها للأمن السيبراني ؟ و هل كان الأمن السيبراني عائقا للهم في استعمال المعلوماتية؟.

الإطار النظري والدراسات السابقة:

مفهوم الأمن السيبراني:

انبثقت عبارة Cyber من أعمال نوربت واينر Weiner Norbert ،عندما حاول تطوير نظريته عن رسائل السبر نتيكا Cybernetics والتي تعود إلى اليونانية ومن مشتقاتها معنى الإدارة والحكم. حيث كان يستهدف ضبط البيئة التي يوجد فيها الكائن والتحكم فيها لملائمة احتجاجاته. (بورياح، 2023 ، ص.274).

أما الأمن السيبراني فهو أمن الفضاء المعلوماتي، وهو تعبير أشمل وأعم من أمن المعلومات. فالمقصود مجموعة من الإجراءات والتدابّر الوقائية التي تؤمن المعلومات " ستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها من السرقة أو الاختراق، ومن زاوية أكاديمية هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات ويضع الأدوات أو الإجراءات اللازمة لضمان حمايتها". وللمحافظة على أمن البيانات والمعلومات في النظام يجب توفر عناصر السرية، التكامل وسالمة المحتوى، التوافر والإتاحة.(البار، المرجي، 2018 ، ص.1-2)

كما يعرف أيضا بأنه "مجموع الوسائل والأدوات والإجراءات اللازم توفرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية". (الخمايسة، 2017 ،ص.288)

وُيعرف الأمن السُبرانً بأنه "مجموع الوسائل التقنية والإدارية التًي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتؤمّن حمأة وسرية وخصوصية البيانات الشخصية ولحماية المواطنين".(البار، المرجي، 2018 ،ص8)

على الرغم من وجود عدة تعريفات للأمن السيبراني، إلا أنها تتمحور في مفهوم توفير الحماية السيبرانية و>لك بغرض ضمان استمرارية توافر النظم المعلوماتية واتخاذ الإجراءات الكفيلة لحماية الأفراد والدول من تلك المخاطر السيبرانية.

أهداف الأمن السيبراني:

يهدف الأمن السيبراني الى حماية البنية التحتية لأمن المعلومات وحماية بيانات المواطنين "وكل ما يتعلق ببيانات المواطنين يحتاج إلى حماية قوية وتخزينها في مكان آمن."(سي عبالقادر،2024، ص.23) وحماية شبكات المعلومات والاتصالات لها الدور الرئيسي في تدفق البيانات بين الأفراد والجماعات مؤسسات ودول وفي حال تعطلها اختراقها أو التشويش عليها فإن ذلك يؤثر مباشرة على التواصل والاتصال وتعطله وبالتالي تعطل الأعمال وتوقف الخدمات .

أبعاد الأمن السيبراني :

البعد العسكري: انبثقت الإنترنت من رحم الحرب الباردة، حيث سعى كل من الاتحاد السوفيتي والولايات المتحدة الأمريكية إلى تطوير تقنيات عسكرية متقدمة تُعزّز من هيبتهم ونفوذهم. فكانت شبكة أربانت (ARPANET) أولى تجليات هذا الصراع، حيث ربطت بين أربعة جامعات أمريكية بهدف تبادل المعلومات العلمية والأبحاث العسكرية. ومع مرور الوقت، تحوّل الإنترنت من أداة حرب إلى منصة معرفية، حيث اتّسعت رقعة مستخدميه لتشمل المؤسسات الأكاديمية والباحثين العلميين من مختلف أنحاء العالم. وفّر الإنترنت بيئة خصبة لتبادل المعرفة والأفكار، ممّا ساهم في تسريع التقدم العلمي والتكنولوجي بشكلٍ ملحوظ. لكن سرعان ما تحوّلت هذه المنصة المعرفية إلى ساحة جديدة للصراعات، حيث ظهرت الجرائم الإلكترونية كتهديدٍ خطيرٍ يهدد الأمن القومي للدول. وتنوّعت أشكال هذه الجرائم لتشمل الاختراقات الإلكترونية وسرقة البيانات وشنّ الهجمات الإلكترونية، ممّا أدى إلى عواقب وخيمة على بعض الدول، كاندلاع نزاع مسلح كما حدث بين روسيا وجورجيا عام 2008، حيث شنّت روسيا هجمات إلكترونية واسعة النطاق على جورجيا، أدت إلى تعطيل البنية التحتية الرقمية للدولة وشلّ قدرتها على الدفاع عن نفسها. قطع الاتصالات: ففي عام 2007، قامت إستونيا بطرد سفير روسيا بعد هجمات إلكترونية واسعة النطاق استهدفت المواقع الحكومية ووسائل الإعلام، ممّا أدى إلى قطع الاتصالات الإنترنت عن جزء كبير من البلاد.

تعطيل الخدمات الحكومية: تعرضت كوريا الجنوبية عام 2013 لهجمات إلكترونية استهدفت البنوك ووسائل الإعلام، ممّا أدى إلى تعطيل الخدمات الحكومية وتكبّد البلاد خسائر اقتصادية فادحة.

استهداف البنية التحتية: في عام 2010، تعرّضت إيران لهجمات إلكترونية استهدفت محطة بوشهر للطاقة النووية، ممّا أثار قلق المجتمع الدولي ودفع إيران إلى تعزيز قدراتها الأمنية الإلكترونية، ومع ازدياد اعتماد الدول على الإنترنت في مختلف جوانب حياتها، أصبحت القدرة السيبرانية عنصرًا هامًا في الاستراتيجيات العسكرية للدول. وتُتيح هذه القدرة للدول ربط وحداتها العسكرية ببعضها البعض من خلال شبكات عسكرية في الفضاء الإلكتروني، ممّا يُعزّز من قدرتها على شنّ هجماتٍ إلكترونيةٍ ضدّ أعدائها، ولكن، تُواجه الدول أيضًا خطر الهجمات الإلكترونية المضادة التي تستهدف شبكاتها العسكرية، ممّا قد يُؤدّي إلى تدمير قواعد البيانات العسكرية وما يتبع ذلك من مخاطر جسيمة، لقد تحوّل الإنترنت من أداة حرب إلى منصة معرفية ومن ثمّ إلى ساحة صراع جديدة. وأصبحت القدرة السيبرانية عنصرًا هامًا في الاستراتيجيات العسكرية للدول، ممّا يُؤكّد على أهمية الأمن الإلكتروني في حماية الدول من التهديدات الرقمية المتزايدة.

2 - البعد القانوني: تُلقي أنشطة الأفراد والمنظمات والحكومات في الفضاء السيبراني بظلالها على الالتزامات والتبعات القانونية التي تتطلب اهتماماً خاصاً. ونظرًا لطبيعة الفضاء السيبراني الديناميكية، تبرز الحاجة إلى حلّ النزاعات التي قد تنشأ عن هذه الأنشطة، مع مراعاة حقوق أخرى مثل الوصول إلى شبكات المعلومات العالمية. وتواجه بعض المفاهيم القانونية تحديات جديدة في ظلّ التحولّات التي صاحبت ظهور مجتمع المعلومات. فقد اتسعت لتشمل نطاقات جديدة مثل الحقّ في إنشاء المدونات والحقّ في تكوين مجتمعات إلكترونية والحقّ في حماية ملكية برامج المعلومات. وتشمل بعض التحديات القانونية في الفضاء السيبراني ما يلي:

تحديد المسؤولية: قد يكون من الصعب تحديد من هو المسؤول عن الأنشطة الضارة في الفضاء السيبراني، خاصةً عندما تنطوي على مشاركة جهات متعددة من دول مختلفة.

وانين الاختصاص: قد تختلف قوانين الاختصاص والقوانين المطبقة على النزاعات الإلكترونية بين الدول، ممّا قد يُعيق عملية حلّ النزاعات بشكلٍ عادلٍ وفعّال.

حماية البيانات الشخصية: تُثير جمع البيانات الشخصية واستخدامها في الفضاء السيبراني مخاوف بشأن الخصوصية وحماية البيانات.

مكافحة الجرائم الإلكترونية: تتطلب مكافحة الجرائم الإلكترونية مثل القرصنة وسرقة البيانات والتشهير الإلكتروني تعاونًا دوليًا وثيقًا وتطوير قوانين فعّالة لمكافحة هذه الجرائم.

ولمعالجة هذه التحديات، هناك حاجة إلى جهود دولية منسّقة لتطوير قوانين ومعايير جديدة تُنظم الأنشطة في الفضاء السيبراني وتُحافظ على حقوق الأفراد والمنظمات والدول. كما يجب تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وتبادل المعلومات والخبرات. وبشكلٍ عام، تُعدّ المسؤوليات القانونية في الفضاء السيبراني مجالًا هامًا يتطلب اهتمامًا خاصاً من قبل الأفراد والمنظمات والحكومات. وفهم هذه المسؤوليات وتطبيقها بشكلٍ فعّال يُساهم في خلق فضاء سيبراني آمن وعادل للجميع.

أهمية الأمن السيبراني:

صبح الأمن السيبراني حاجةً ملحةً لا غنى عنها في ظلّ انتشار التهديدات الإلكترونية التي تستهدف البيانات الحساسة للمؤسسات والأفراد. وتسعى هذه الهجمات إلى الوصول إلى تلك البيانات أو حذفها أو التحكم بها، ممّا يُهدّد الأمن القومي والخصوصية والاستقرار الاقتصادي، ولقد ازدادت أهمية الأمن السيبراني بشكلٍ كبيرٍ مع ظهور الثورة الصناعية الرابعة، أو ثورة البيانات. حيث تعتمد هذه الثورة بشكلٍ كبيرٍ على الأنظمة الرقمية والشبكات المترابطة، ممّا يُتيح مجالات واسعة للمخترقين والمجرمين الإلكترونيين.

ويهدف الأمن السيبراني إلى مواجهة هذه المخاطر من خلال حماية الأنظمة والبيانات من الوصول غير المصرح به والاختراقات الإلكترونية وهجمات البرامج الضارة. كما يُساهم في ضمان استمرارية عمل المؤسسات وحماية المعلومات الشخصية للمستخدمين، ومن أهمّ المخاطر التي تواجه الفضاء السيبراني الجريمة الإلكترونية، والتي تشمل مجموعة واسعة من الأنشطة

مثل القرصنة وسرقة البيانات والابتزاز الإلكتروني والتشهير عبر الإنترنت. وتُعدّ هذه الجرائم تهديدًا خطيرًا للأفراد والمؤسسات على حدٍ سواء، ممّا يتطلب جهودًا متضافرة لمكافحتها، ولذلك، أصبح الأمن السيبراني مسؤوليةً مشتركةً تقع على عاتق الجميع.

أنواع الأمن السيبراني:

هناك أنواع متعددة مختلفة من الأمن السيبراني منها

النوع الأول: أمن الشبكات Network Security والمتمثل في الهجوم على الشبكات الالكترونية، وعليه فالأمن السيبراني هو الحل الأمثل لحماية كافة شبكات الحاسوب من الهجمات وهو الذي يتيح التحكم في البيانات وحمايتها من الهجوم والسرقة

النوع الثاني: الأمن السحابي Cloud Security. ونظرا لصعوبة الاحتفاظ بالكم الهائل من البيانات ولذلك تعمل العديد من المؤسسات و الشركات على توفير أفضل الخدمات المساعدة على توفير الخدمات في زمن قياسي ومن بينها على سبيل المثال قوقل كلود وميكروسوفت أزير.

النوع الثالث: أمن التطبيقات فالتطبيقات مرتبطة بشبكة الانترنت يتم اختراقها والسطو على بياناتها وهنا تأتي اهمية الأمن السيبراني اذ يمكن من أي هجوم محتمل للأفراد أو الشركات

النوع الرابع: الامن التشغيلي "إن تم تعرض البيانات إلى الاختراق هنا يساعد هذا النوع على في الوصول إلى العديد من الخطط البديلة لذلك يتم الاعتماد عليه في أغلب الشركات والمؤسسات الضخمة، مع شركة النور أون لاين سوف نقدم أفضل الخدمات حتى يتم الحفاظ على كافة البيانات والمعلومات الخاصة بالعملاء"https://www.elnooronline.net/.

الإطار المنهجي:

1 - منهج الدراسة: يتحدد منهج الدراسة حسب طبيعة المشكلة المدروسة وخصائصها ، وقد استعملنا في دراستنا الحالية المنهج الوصفي الاستكشافي كوننا بصدد وصف الظاهرة وجمع الملاحظات والحقائق والمعلومات عنها وتقرير حالتها كما هي عليه في الواقع وهذا المنهج هو الأنسب لمثل هذه الدراسات.

2 - مجتمع وعينة الدراسة : استعملنا في دراستنا هذه عينة حصصيه ممثلة في أساتذة التعليم الثانوي، تكونت الدراسة من ثمانية وعشرون أستاذا (28) من أساتذة التعليم الثانوي من مجموع 42 أستاذا للتعليم الثانوي بثانوية ديدي صالح، حيث مثلت العينة نسبة66.66% من أساتذة الثانوية.

3 - أدوات الدراسة :استخدمنا في دراستنا هذه المقابلة لما تكتسيه هذه الأداة من أهمية ولما لها من صدق وموضوعية في جمع البيانات، وقد تكونت المقابلة من أربعة اسئلة مفتوحة: الأول عن مدى استعمال و توظيف الذكاء الاصطناعي في التعليم لدى أساتذة التعليم الثانوي ، والثاني عن نوعية برامج الذكاء الاصطناعي المستعملة من طرف الأساتذة، والثالث عن مدى فائدة هذه البرامج لهم، والرابع عن الصعوبات التي تواجه الأساتذة في استعمال الذكاء الاصطناعي وقد أجريت المقابلة مع اساتذة التعليم الثانوي بعد تحديد الفترة المناسبة وهي من 05 مارس2024 الى غاية 05 أفريل 2024.

4 - الأساليب الإحصائية المستخدمة : اعتمدنا في دراستنا هذه على أسلوب الاحصاء الوصفي نظرا لأنه المساعد في جمع المعلومات والبيانات حول موضوع الدراسة، ثم القيام بتنظيم المعلومات والبيانات وترتيبها وتبويبها وذلك بحساب التكرارات والنسب المؤية.

عرض و مناقشة النتائج:

1 - عرض و تحليل ومناقشة نتائج التساؤل الأول:

الجدول (01): حاجة وإحساس أساتذة التعليم الثانوي بضرورة الأمن السيبراني

العدد	نعم	النسبة	لا	النسبة	بدون اجابة	النسبة
28	**25**	**% 89.28**	**02**	**% 07.14**	**01**	**% 03.57**

بعد جمعنا للبيانات من ثمانية وعشرون أستاذا للتعليم الثانوي حول احساسهم بضرورة الأمن السيبراني، قمنا بتلخيص ذلك في من خلال الجدول رقم (01) وإجابة على التساؤل الأول هل يحس أساتذة التعليم الثانوي بالحاجة الى الأمن السيبراني؟ تلاحظ ان نسبة كبيرة من الأساتذة يحسون بضرورة الأمن السيبراني بنسبة قدرت ب89.58% وهو مؤشر يدل ضرورة وجود حماية من التهديدات والمخاطر والجرائم الإلكترونية المتسارعة وهو ما أشارت اليه الراسات السابقة كدراسة(قطاف، 2022) و(مسيكة، 2022) و(بوقرص،2022). وما نلاحظه من الجدول رقم (01)النسبة الضعيفة للأساتذة الذين لا يشعرون بالحاجة الى الأمن السيبراني، بسبب عدم ولوجهم الى عالم الرقمنة وعم ممارستهم لتكنولوجيا الوسائل الرقمية وهو مؤشر سلبي رقم ضعف النسبة فالأستاذ يمثل أحد الشرائح الرائدة في مجتمع يطمح الى التطور والرقي في عالم اصبح التكنولوجيا الرقمية أهم اركانه.

2 - عرض و تحليل ومناقشة نتائج التساؤل الثاني:

الجدول (02): مجالات حاجة أساتذة التعليم الثانوي للأمن السيبراني

	المجال	التكرار	النسبة
01	**البرامج التي تخزن المعلومات الشخصية**	**10**	**% 34.71**
02	**مواقع التواصل الاجتماعي**	**07**	**% 25.00**

03	بطاقات التداول الالكترونية	05	% 17.85
04	المجال التربوي وقطاع التعليم	05	% 17.85
05	مجال التجارة الالكترونية	03	% 10.71
06	مجال امن جهاز الحاسوب	03	% 10.71
07	اشتراكات المواقع الالكترونية	02	% 07.14
08	البحث العلمي	02	% 07.14
09	الرقمنة المدرسية	02	% 07.14

من خلال الجدول رقم (02) نلاحظ أن أكثر المجالات التي يحتاج فيها أسات>ة التعليم الثانوي للأمن السيبراني هو مجال البرامج التي تخزن المعلومات الشخصية بنسبة 34.71 % ثم مجال مواقع التواصل الاجتماعي بنسبة 25.00% ثم مجالي بطاقات التداول الالكترونية والمجال التربوي وقطاع التعليم بنسبة متشابهة 17.85 %، ثم مجال التجارة الالكترونية و مجال امن جهاز الحاسوب بنسبة 10.71 % وأخيرا مجال اشتراكات المواقع الالكترونية ومجال البحث العلمي ومجال الرقمنة المدرسية بنسبة هي الأضعف07.14 % ، وهو ما يدل على أن أساتذة التعليم الثانوي كوتهم شريحة من المجتمع لازال عدم أمن المعلومات الشخصية يشكل هاجسا كبيرا لديهم بحكم التكنولوجيا الرقمية بالقدر الذي تقدم فيه خدمات رائدة وبجهد أقل ووقت وجيز فإنها من ناحية أخرى مثلما أشارت العديد من الدراسات تشكل تهديدا لأمن الأفراد والمجتمعات والدول.

3 - عرض و تحليل ومناقشة نتائج التساؤل الثالث:

الجدول (03): هل كان عدم الأمن السيبراني عائق أمام استعمال المعلوماتية

نعم	النسبة	لا	النسبة
06	% 21.42	21	% 75.00

يمثل الجدول رقم (03) اجابة على التساؤل هل كان عدم الأمن السيبراني عائق أمام استعمال المعلوماتية؟ ومن خلاله نلاحظ أن نسبة75.00 % من أساتذة التعليم الثانوي لم يكن عدم الأمن السيبراني عائقا لهم أمام استعمال المعلوماتية، وهذا ما يدل على أنه وبرغم المخاطر المحتملة والتهديدات والابتزازات الإلكترونية الا أن الولوج الى عالم المعلوماتية بقات أمر ضروري في علم يوصف بأنه رقمي، في حين شكلت نسبة 21.42 % من الأساتذة نسبة الأساتذة الذين كان عدم الأمن السيبراني عائقا لهم أمام استعمال المعلوماتية ومن الأمثلة لعدم استعمال المعلوماتية بسبب عدم الامن السيبراني عدم استعمال المواقع التي تتطلب صلاحيات الدخول للمعلومات الشخصية
عدم الولوج للمواقع التي تتطلب الدفع للحصول على المعلومات أو الكتب أو الأبحاث.

خلاصة:

توصلت دراستنا الى النتائج التالية: نسبة 89.28 % من أساتذة التعليم الثانوي يحسون بالحاجة الى الأمن السيبراني، ومن أهم المجالات الي يحتاجون فيها للأمن السيبراني البرامج التي تخزن المعلومات الشخصية، مواقع التواصل الاجتماعي، بطاقات التداول الالكترونية و المجال التربوي وقطاع التعليم ونسبة 75% منهم لم يكن عدم الأمن السيبراني عائقا لهم في استعمال المعلوماتية.

إن الأمن السيبراني يمثل ممارسة أساسية لحماية الشبكات، الأجهزة، التطبيقات، الأنظمة، والبيانات من مخاطر الفضاء الإلكتروني. ويهدف بشكل رئيسي إلى صدّ الهجمات الخبيثة التي تسعى إلى الوصول إلى البيانات الحساسة أو إتلافها، أو ابتزاز الأموال، أو حتى تعطيل العمليات التجارية، وهو ليس مجرد خيارٍ بل ضرورة ملحة في ظلّ ازدياد التهديدات الرقمية وتطورها بشكلٍ مستمر ولذلك يُعدّ الأمن الإلكتروني مسؤولية مشتركة تقع على عاتق الأفراد والمؤسسات على حدٍ سواء، ويجب اتباع نهج استباقي يشمل مجموعة من الإجراءات الوقائية مثل:

استخدام كلمات مرور قوية وفريدة من نوعها وتثبيت تحديثات البرامج بانتظام و توخي الحذر عند فتح رسائل البريد الإلكتروني المشبوهة أو النقر على الروابط غير الموثوقة و استخدام برامج مكافحة الفيروسات والبرامج الضارة مع الاحتفاظ بنسخ احتياطية من البيانات المهمة ثم تدريب الموظفين على ممارسات الأمن الإلكتروني الجيدة.

وبناء على هذه النتائج وبناء على الدراسات السابقة نقدم مجموعة توصيات:

- تحديث السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات بما يسمح وتوفير خدمات جديدة ومتطورة للمواطنين والمؤسسات بما فيها المؤسسات التربوية.
- خلق بيئة مشجعة داعمة للشباب من أجل الاستثمار في تطوير وتوسيع الشبكات والاتصالات.
- تعزيز التعاون بين القطاع العام والقطاع الخاص في تبادل المعلومات ووجهات النظر والتدريب ودراسة مواطن الضعف والقوة.
- خلق تخصصات جامعية في العلوم الإنسانة والاجتماعية والعلوم التكنولوجية لمواكبة التطورات المتسارعة في هذا التخصص.
- تنظيم الندوات وورشات العمل بالتعاون بين الجامعات والمؤسسات الوطنية والدولية ذات الصلة بالآمن السيبراني من أجل تبادل الخبرات.
- العمل على رفع الوعي المجتمعي بالمخاطر السيبرانية، والعمل من أجل ضمان الاستخدام المسؤول والآمن للتكنولوجيات الحديثة والتطبيقات الرقمية الحديثة.

المراجع:

- الخمايسة، صدام محمد طالب.(2017). *الحكومة الذكية ما بعد الحكومة الإلكترونية*، قنديل للطباعة والنشر والتوزيع.
- البار، عدنان مصطفى والمرجي، خالد علي(2018). أمن المعلومات والأمن السيبراني. https://bit.ly/30h2jom
- بورياح، سلمة(2023). السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات. *مجلة دفاتر السياسة والقانون*، 15(01)، EISSN : 0220-5222 ISSN : 1112-9808.291-273
- بن برغوث، ليلى.(2023). الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصرالتحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات وآليات التصدي. *المجلة الدولية للاتصال الاجتماعي*،10(01)، 443- 457..ISSN:2437-1184
- مسيكة، محمد(2022). الفضاء السيبراني وتحديات الأمن القومي للدول. *مجلة العلوم القانونية و الاجتماعية*، 447- 462. Issn: 2507-7333 Eissn: 2676-1742
- بوقرص، ساعد(2022). الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة. *مجلة الأبحاث في الحماية الاجتماعية*، 03(01)، 61-77، 2772-3009 : EISSN/2716-8182ISNN.
- قطاف، سليمان(2022). الأمن السيبراني والمضامين المفاهيمية المرتبطة به، *مجلة طبنة للدراسات العلمية الأكاديمية*، 05(02)، 37-56. ISSN 2661-7633 / EISSN 2716-8883
- سي عبد القادر، حنان(2024). الأمن السيبراني و أثره على دول العالم، *مجلة البصائر للدراسات القانونية والاقتصادية*، 04(07)، 21-37. ISSN : 2773-3378
- بارة، سمير(2017). الأمن السيبرانيCyper Security السياسات والمؤسسات، *المجلة الجزائرية للأمن الإنساني*، 04 ISSN: 2543-375X .