جامعة غليزان
RELIZANE UNIVERSITY

جامـــــــــعة غليـزان

كلية العلـوم الاجتمـاعية والإنسانية

أطروحـــــــة

للحصول على شهـــــادة دكتوراه ل. م. د

في علم الاجتماع جريمة وانحراف

مستوي الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الألكترونية

دراسة ميدانية بكلية العلوم الإنسانية والاجتماعية بجامعة الجيلالي بونعامة – خميس مليانة–

مقدمة ومناقشة علنا من طرف

السيد(ة): برادة عبد الرزاق

أمام لجنـــــــة المناقشـــــــة

اللقب والاسم	الرتبـــــة	المؤسسة الأصلـــية	الصـــــفة
بن حميدة هند	أستاذ التعليم العالي	جامعة غليزان	رئيـــــسا
سالي مراد	أستاذ محاضر أ	جامعة خميس مليانة	مشرفا ومقـــــررا
صيشي يسري	أستاذ محاضر أ	جامعة شلف	مشرفا ثانيا
بطاوي بهية	أستاذ محاضر أ	جامعة غليزان	منـــاقشا
درامشية لمياء	أستاذ محاضر أ	جامعة غليزان	منـــاقشا
بن يوب محمد	أستاذ التعليم العالي	جامعة تلمسان	منـــاقشا
بن شرقي عبد الاله	أستاذ محاضر أ	المركز الجامعي بمغنية	منـــاقشا

السـنة: 2024/2023

الإهـــداءُ

❀❀❀إلى التي أعطتني ولم تبخل❀❀❀

إلى التي أنارت لي الدرب بالشموع

إلى التي وهبت لي حياتها **أمي رمز الحنان.**

إلى أحلى كلمة يرددها لساني إلى أجمل كائن عرفته عيوني **أبي العزيز**

إلى كل إخوتي وأخواتي الذين بهم تلتئم جراحي.

إلى جميع الأهل والأقارب.

إلى رفيقين المشوار الذي ساعداني في إنجاز هذه الأطروحة: **مصطفي المغاني**

وفتحي القصير

إلى كل الأصدقاء والزملاء في مخبر الدارسات الاجتماعية والنفسية

والأنثروبولوجيا بجامعة غليزان

وفي الأخير إلى كل من كان ساندي في الحياة وعشت معهم أحلى أوقاتي وتمنى

❀❀❀لي النجاح❀❀❀

❀❀❀

شكر وتقدير

بسم الله الرحمان الرحيم

الحمد لله رب العالمين والصلاة والسلام على المبعوث رحمة للعالمين سيدنا محمد وآلة وصحبه أجمعين عملا بقوله تعالى" **وإذا تأذن ربك لإن شكرتم لأزيدنكم .....**"

نشكر الله على نعمه التي لا تقدر ولا تحصى ومنها توفيقه تعالى على إتمام هذا العمل نتقدم بجزيل الشكر والامتنان وخالص العرفان والتقدير للدكتورين **أبي وأمي** الذين شرفاني بقبول الإشراف على هذه الأطروحة وعلى دعمهما وتوجيهاتهما القيمة فجزاهم الله خير الجزاء دون أن ننسي تعزينا الخالصة لعائلة مشرفي الأول **د. مهدي قصير** رحمه الله واسكنه فسيح جناته وغفر له وجعل قبره روضة من رياض الجنة.

كما يسرنا أن نوجه أسمى آيات التقدير والعرفان إلى رئيس المشروع **د.بغداد باي عبد القادر** على دعمه وتوجيهاته القيمة لكل طلبة الدكتوراء و صديقي **مصطفي المغاني** الذي ساعدني في انجاز الأطروحة.

كما نتقدم بخالص الشكر والعرفان إلى موظفي المكتبات داخل الجامعة وخارجها وكل من ساعدنا في هذا العمل، كما نشكر أيضا **عميد كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة ونائبه** على حسن استقبالهم لنا وتسهيل لي في أجراء الدراسة.

وقبل وبعد فالشكر لله ولله الحمد في الأول والأخير.

"مستوي الوعي السيبر اني في الوسط الجامعي وعلاقته بالجريمة الألكترونية"

ملخص:

هدفت هذه الدراسة إلى فهم العلاقة بين الوعي السيبراني والوعي بالجريمة الألكترونية في الجامعة الجزائرية وتحديداً بالنسبة لطلبة كلية العلوم الاجتماعية والإنسانية في جامعة خميس مليانة، حيث يبلغ عددهم 355 طالب وطالبة تم اعتماد منهج وصفي الارتباطي لإجراء هذه الدراسة، وتم استخدام الاستبيان كأدت بحثية، وبشكل خاص تم توزيع استبيان على عينة الدراسة التي تتألف من 355 فردًا، وهو ما يمثل حوالي 38.47% من مجموع الفئة المستهدفة وقد خلصت الدراسة الى جملة من النتائج أهمها:

1. استنتجنا من وجه نظر الطلبة أن الوعي السيبراني مهم في تحقيق أمنهم من الجريمة الألكترونية عند أستخدم الأنترانت.
2. وجود مستوي متوسط في الوعي السيبراني لطلبة كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة.
3. وجود مستوي متوسط في الوعي بالجريمة الألكترونية لطلبة كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة.
4. عدم وجود فروق ذات دلالة إحصائية في استجابات المبحوثين حول الوعي السيبراني تعزي للمتغيرات: (الجنس، السن، والمستوي التعليم) بينما توجد فروق في متغير القسم لصالح قسم العلوم الإنسانية.
5. عدم وجود فروق ذات دلالة إحصائية في استجابات المبحوثين حول الوعي بالجريمة الألكترونية تعزي للمتغيرات: (السن، والمستوي التعليم) بينما توجد فروق في متغير القسم لصالح قسم العلوم الإنسانية الى فروق وفق متغير الجنس لصالح الإناث.
6. وجود علاقة ارتباطية بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة.

وقدمت الدراسة مجموعة من التوصيات أبرزها عقد دورات في تنمية مهارات الأمن السيبراني وملتقيات وطنية وندوات حول مخاطر الجريمة الألكترونية وتفعيل دور الأدارة الأمن السيبراني داخل الجامعة للحد من التهديدات السيبرانية التي تواجه أفراد الوسط الجامعي.

"**Cyber Awareness Level in Algerian Universities and Its Relationship with Cybercrime**"

Abstract:

This study aimed to comprehend the relationship between cyber awareness and awareness of electronic crime among students at the University of Khemis Miliana, specifically those enrolled in the Faculty of Social and Human Sciences, where the total number of students was 355, A descriptive correlational approach was employed for this study, utilizing a questionnaire as a research tool. The questionnaire was distributed to a study sample consisting of 355 individuals, representing approximately 38.47% of the target population. The study yielded several key results:

1. From the students' perspective, it was inferred that cyber awareness is crucial in safeguarding them against electronic crime when using the internet.
2. There exists a moderate level of cyber awareness among students of the Faculty of Social and Human Sciences at the University of Khemis Miliana.
3. A similar moderate level of cyber crim was found among students of the Faculty of Social and Human Sciences at the University of Khemis Miliana.
4. There were no statistically significant differences in respondents' responses regarding cyber awareness related to variables such as gender, age, and education level. However, differences were observed based on the department, favoring the Department of Humanities.
5. Similarly, there were no statistically significant differences in respondents' responses regarding awareness of electronic crime based on age and education level. However, differences were observed based on

the department, favoring the Department of Humanities, as well as gender, favoring females.

6. A correlational relationship was identified between the level of cyber awareness among students of the Faculty of Social and Human Sciences at the University of Khemis Miliana and their awareness of electronic crime, as perceived by the students.

The study provides a set of recommendations, including the organization of courses to enhance cyber security skills, national conferences and seminars on the risks of electronic crime, and the activation of the role of cyber security management within the university to mitigate cyber threats faced by members of the academic community.

الفهرس

فهرس الجداول

فهرس الملاحق

مقدمة

مقدمة:

يعتبر التقدم التكنولوجي في مجال نقل المعلومات من خلال الإنترنت من أبرز الظواهر الحديثة التي شهدت انتشارًا واسعًا. أفاد التقرير العلمي لمكتب الأمم المتحدة (2013) بأن عدد الأشخاص الذين يتصلون بالإنترنت زاد منذ عام 2011، حيث ارتفع عدد المستخدمين من 2.4 مليار ليصل إلى 60 في المئة، معظمهم من دول في طور النمو. هذا يعكس الانتشار الواسع للإنترنت وعدم اقتصارها على الدول المتقدمة فقط، نظرًا لأسعارها المعقولة التي تسمح للأفراد بشرائها مع الحاسوب كونه جهازًا أساسيًا لتحقيق التفاعل مع الفضاء الافتراضي (UNODC، 2013).

برز، من خلال هذا التقدم التكنولوجي، مجال مكاني جديد للتفاعل الاجتماعي يعرف بالفضاء الإلكتروني، حيث يجتمع الأفراد وتغيب فيه الحدود المادية والاجتماعية. يُعتبر هذا الفضاء مرحلة انتقالية للإنسان من العالم الواقعي إلى العالم الافتراضي، مما أدى إلى انتقال العديد من الظواهر وتدفق العديد من التغييرات التي أثرت على مجال التعليم العالي والوسط الجامعي. أنتجت التكنولوجيا العديد من المفاهيم الجديدة والفروق الاجتماعية مثل الاختلافات بين متصلين وغير متصلين بالإنترنت، الحقيقة والافتراضية، المادية وغير المادية.

إضافة إلى ذلك، ظهرت العديد من المفاهيم التي رافقت الرقمنة في التعليم العالي مثل الجودة الرقمية، والتعليم الإلكتروني، والأدوات الإلكترونية، والهوية الرقمية، والوعي الرقمي، وغيرها. ومن بين التغييرات التي أحدثها التحول الرقمي في الجامعة، كان هناك تأثير كبير على جودة التعليم العالي. فكلما اعتمدت الجامعة على تكنولوجيا المعلومات في تسيير مؤسساتها وتنظيم التفاعل داخل الهيكل التنظيمي، والاعتماد على الإنترنت في التواصل الداخلي والخارجي، أصبحت مؤسسة ذات تكوين راقٍ من حيث حداثة المادة العلمية وأساليب التكوين الأكاديمي.

نتيجة لهذا التقدم التكنولوجي والانتشار الواسع للإنترنت، أصبح من الضروري التفكير في الوعي السيبراني لمجتمع الجامعة الجزائرية. هذا الموضوع يحظى باهتمام واسع من باحثين وأكاديميين دوليين ومحليين في تخصص العلوم الاجتماعية، حيث فُرضت عليهم الهجرة من الواقع المادي في مجال البحث العلمي، والتوجه نحو دراسة الظواهر المنتشرة في العالم الافتراضي من خلال التركيز على التحول والتغيير في الوسط الجامعي. فقضية الوعي السيبراني قد رافقت تحول الجامعة الجزائرية والتعليم الأكاديمي نتيجة اعتماد الإنترنت في التعليم العالي الجزائري.

لذا، أصبح الوعي السيبراني بالنسبة للمكونات المادية والبشرية للوسط الجامعي الجزائري أمرًا ضروريًا بسبب الفضاء الإلكتروني الذي ينتج في جانبه السلبي أنواعًا جديدة من الجرائم تُسمى بالجرائم الإلكترونية. وقد خلقت هذه الجرائم فرصًا جديدة للمجرمين، مكنتهم من تصفح الإنترنت وارتكاب جرائم مثل اختراق المواقع والأشخاص، الاحتيال، التلاعب بمعلومات مؤسسات الدولة، ونشر المواد الإباحية، مما يجعل من الصعب ملاحقتهم أو الكشف عن الجرائم.

مع ذلك، يجب معالجة موضوع مستوى الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية، وكشف التغييرات التي طرأت على الوسط الجامعي الجزائري، خاصةً في ضوء الرقمنة التي تشهدها المؤسسات الجامعية، حيث تحولت البنية المادية إلى نظام معلوماتي يُخزن فيه كل المعلومات باستخدام الإنترنت. هذا يتطلب من الطلاب والطالبات في الجامعة تحقيق الاستخدام الآمن للإنترنت، حيث يمكن لأي خطأ في التعامل مع المحتوى الرقمي، مثل تحميل المستندات والمحاضرات والدخول إلى مواقع الإنترنت الرسمية للجامعة، أن يعرض أجهزتهم لهجمات إلكترونية أو جرائم سيبرانية.

بناءً على هذا الأساس، تهدف دراستنا الحالية إلى معرفة مستوى الوعي السيبراني ومستوى الوعي بالجريمة الإلكترونية والعلاقة بينهما لدى طلاب كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة. بالإضافة إلى ذلك، تسعى الدراسة لتحديد الفروق في استجابات الطلاب في كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة، وذلك من أجل الإلمام بكل أبعاد الدراسة والإجابة على التساؤلات المطروحة والفرضيات المقترحة. قمنا بتصميم هيكل للدراسة يتضمن أربعة فصول يمكن تلخيصها كالتالي:

الفصل الأول: الإطار المنهجي للدراسة، حيث يتضمن تقديم المشكلة البحثية وشرح مختلف المتغيرات التي سيتم دراستها وتحليلها ميدانيًا. يشمل أيضًا تقديم الأسئلة البحثية والفرضيات المقترحة وتحديد الأهداف والأهمية العلمية للبحث، وعرض المفاهيم الأساسية والدراسات السابقة المتعلقة بموضوع الدراسة، مع تقديم مقدمة نظرية للموضوع.

الفصل الثاني: يتناول الجريمة الإلكترونية والوسط الجامعي، ويقسم إلى ثلاثة مباحث رئيسية تتعلق بتعريف الجريمة الإلكترونية وأنواعها وتأثيراتها. يتناول أيضًا التقنيات المستخدمة في الجريمة الإلكترونية، تحديات الأمان الإلكتروني، الأسباب التي تجعل الأفراد ضحايا للجريمة الإلكترونية، واستراتيجيات الوقاية من جرائم الإنترنت. كما يستعرض الوسط الجامعي من حيث مفهومه ومكوناته وأهدافه وتدابير الحماية من الجريمة الإلكترونية.

الفصل الثالث: يستعرض الوعي السيبراني في الوسط الجامعي الجزائري، ويقسم إلى ثلاثة مباحث أساسية تتعلق بمفهوم التحول الرقمي في الوسط الجامعي الجزائري وأنواعه وأدواته، الهوية الرقمية للمؤسسة الجامعية وأفرادها، وجهود الجامعات الجزائرية ووزارة التعليم العالي نحو التحول الرقمي ومجال الأمان السيبراني. يستعرض أيضًا الوعي السيبراني للجريمة الإلكترونية وكيفية إدارة الأمان السيبراني داخل الحرم الجامعي.

الفصل الرابع: يقدم الإطار المنهجي والميداني للدراسة، من خلال شرح منهج البحث ومجالاته، مع الإشارة إلى المجتمع المستهدف وأساليب جمع البيانات وتحليلها وتقييم صدقها وثباتها. يتناول أيضًا العينة والأساليب الإحصائية المستخدمة في معالجة البيانات الميدانية، وفي الأخير، يتم تحليل ومناقشة أسئلة الدراسة وعرض نتائجها الجزئية والعامة.

الفصل الأول:

الإطار النظري والتصوري للدراسة

I. الفصل الأول: الإطار النظري والتصوري للدراسة

1. مشكلة الدراسة
2. أسئلة الدراسة
3. فرضيات الدراسة
4. أهداف الدراسة
5. أهمية الدراسة
6. أسباب اختيار الموضوع
7. مفاهيم الدراسة
8. الدراسات السابقة
9. مدخل النظري للموضوع

1.اشكالية الدراسة

شهد العالم تطورًا سريعًا في تكنولوجيا الحواسيب والأجهزة الإلكترونية، وأحدثت تغييرات عميقة في حياة الأفراد وعمل المؤسسات. نتيجة لذلك، أصبح من الضروري استخدام كل من الحاسوب الشخصي والهاتف وتقنياتهم بناءً على أهميتهم في مختلف المجالات والاختصاصات. يبرز هذا بوضوح في مجال البحث العلمي والتعليم العالي في الجزائر، حيث تتطلبها المؤسسات الجامعية لتخزين البيانات الأساسية والمهمة عبر الشبكات الإلكترونية، التي تتألف من الإنترنت وأنظمة الكمبيوتر والمعلومات الرقمية.

وفي هذا السياق، تعتبر التهديدات السيبرانية من أهم المخاطر التي تواجه الشبكات الإلكترونية للمؤسسات مثل الجامعة. إذ تتعرض هذه الشبكات ومواردها البشري من طلبة وأساتذة وموظفين للتهديدات السيبرانية بناءً على التطور السريع لهذه التهديدات، مقارنةً بتطور الجانب الأمني المكلف بمواجهتها. حيث عرفت الفترة الممتدة بين سنة 2022 و2023 تسجيل أكثر من 4600 قضية جريمة إلكترونية في الجزائر، شملت الابتزاز والتهديد والتشهير والمساس بالحريات الشخصية والحياة الخاصة عبر مواقع التواصل الاجتماعي. بالإضافة إلى جرائم نشر المعلومات الزائفة والمضللة، والقرصنة والتشهير والتحرش الإلكتروني والنصب والاحتيال. وقد تراوحت نسبة القضايا التي تتعلق بحياة الأفراد بين 65٪ و75٪ من القضايا المعالجة، وذلك وفقًا لحصيلة الدرك الوطني الجزائري (الشروق، 2023).

ويعزى ظهور هذا النوع من الجرائم في الجزائر إلى التحول الرقمي الذي تشهده البلاد. إذ أشارت تقارير عديدة، منها تقرير We Are Social & Meltwater (2023)، إلى الوضع الرقمي في الجزائر في عام 2023، حيث أظهرت أن هناك 32.09 مليون جزائري يستخدمون الإنترنت بنسبة انتشار تصل إلى 70.9٪. وعلى الجانب المقابل، بلغ عدد مستخدمي وسائل التواصل الاجتماعي 23.95 مليون مواطن، أي بنسبة 52.9٪ من إجمالي السكان. كما يُعتبر الطلاب الجامعيون من فئة الشباب المعروفة بشدة استخدام الإنترنت في التواصل الاجتماعي وإنجاز البحوث العلمية والتعلم عن بُعد وتنزيل الدروس والمحاضرات من المنصات التعليمية الجامعية. يضاف إلى ذلك، أن العديد من هؤلاء الطلاب يقضون وقتًا طويلاً على الإنترنت، بما يصل إلى درجة الإدمان، مما يؤدي إلى آثار نفسية واجتماعية (الضبان وآخرون، 2019، ص 269).

ونظرًا لاستخدام الإنترنت في جوانب متعددة من حياة طلبة الجامعة الجزائرية، فإنهم يكونون عرضة لأنواع معينة من الجرائم الإلكترونية مثل سرقة بياناتهم، واختراق أجهزتهم وهواتفهم أو مواقع التواصل الاجتماعي الخاصة بهم. يتضح من ذلك أهمية الوعي السيبراني في حماية معلوماتهم الشخصية والبيانات الرقمية. علاوة على ذلك، يتعين على الطلبة التمييز بين المعلومات الحقيقية والمصادر الموثوقة التي تكون على شكل مواقع أو أشخاص، حيث يتعرضون لكثير من المحتالين والمعلومات المضللة التي تشكل تهديدًا عليهم. ومع انعدام وعيهم بالجريمة الإلكترونية ومخاطرها الناتجة عن الاستخدام غير الواعي للإنترنت، يزيد من احتمالية أن يكونوا ضحايا لها. وبالتالي، تتحدد مشكلة دراستنا من خلال الإجابة عن التساؤل الرئيسي التالي: "هل لمستوى الوعي السيبراني لطلبة كلية العلوم الإنسانية والاجتماعية في جامعة جيلالي بونعامة علاقة بمستوى وعيهم بالجريمة الإلكترونية؟".

2.أسئلة الدراسة

يحاول البحث الإجابة عن السؤال الرئيسي التالي: ما العلاقة بين الوعي السيبراني والوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة؟ ويتفرع منه الأسئلة التالية:

أ- ما هو الوعي السيبراني والجريمة الإلكترونية من وجهة نظر طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة؟

ب- ما درجة الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة؟

ت- ما درجة الوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة؟

ث- هل توجد فروق في مستوى الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة من وجهة نظر الطلبة تعزى إلى كل من متغيرات الجنس، السن، القسم، والمستوى التعليمي؟

ج- هل توجد فروق في مستوى الوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة من وجهة نظر الطلبة تعزى إلى كل من متغيرات الجنس، السن، القسم، والمستوى التعليمي؟

ح- هل توجد علاقة ارتباطية بين مستوى الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة؟

3.فرضيات الدراسة

أ- الفرضية الأولى: لا توجد علاقة ارتباطية بين مستوى الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة.

ب- الفرضية الثانية: لا توجد فروق ذات دلالة إحصائية في مستوى الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة من وجهة نظر الطلبة تعزى إلى متغيرات (الجنس، السن، القسم، المستوى التعليمي).

ت- الفرضية الثالثة: لا توجد فروق ذات دلالة إحصائية في مستوى الوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة من وجهة نظر الطلبة تعزى إلى متغيرات (الجنس، السن، القسم، المستوى التعليمي).

4.أهمية الدراسة

لكل بحث ودراسة أكاديمية أهميتها العلمية التي تدفع الباحث للسير في أغوارها ومحاولة الوصول إلى نتائج تجيب على تساؤلاته من خلال استخدام المنهج البحثي العلمي وأدواته. وتبرز أهمية هذه الدراسة من خلال:

أ- تناولها لموضوع هام يتمحور حول الوعي السيبراني والجريمة الإلكترونية، التي تعتبر من الجرائم المستحدثة والتي تهدد المجتمع بحكم الاستخدام الواسع للإنترنت في حياتنا اليومية. الوعي السيبراني وإدراكه يرتبطان بمجال الأمن السيبراني، حيث أصبح من الضروري على مستخدمي الإنترنت امتلاك المعرفة الأساسية لتحقيق أمنهم.

ب- تأتي هذه الدراسة نظرًا لصعوبة متابعة مرتكبي الجرائم السيبرانية، كونهم يمتلكون مهارات وقدرات تكنولوجية عالية ويعدون من الفئة المحترفة في مجال البرمجة، مما يشكل تهديدًا على مستخدمي الإنترنت من الطلبة.

ت- تهتم هذه الدراسة بطلبة الجامعة، وهم يعدون فئة جديرة بالاهتمام والدراسة كونهم إطارات المستقبل وسواعد التنمية الاقتصادية والاجتماعية. كما أنهم يمثلون الفئة المثقفة في المجتمع، التي يمكن من خلالها قياس المستوى العام للوعي السيبراني والجريمة الإلكترونية.

ث- تحاول الدراسة لفت انتباه الباحثين إلى إجراء المزيد من الدراسات في مجال الوعي السيبراني والجريمة الإلكترونية والظواهر المنتشرة في الواقع الافتراضي وكل ما يرتبط باستخدام الوسائط الإلكترونية.

ج- تهدف الدراسة إلى تعميم نتائجها وتوصياتها ليستفيد منها الباحثون والمتخصصون، من خلال تناول موضوع الدراسة من زوايا بحث حديثة وإعداد أدواتهم البحثية في دراسات ترتبط بموضوع الجريمة الإلكترونية والوعي السيبراني في مجال علم اجتماع الجريمة والانحراف.

5.أهداف الدراسة

تهدف الدراسة إلى تحقيق مجموعة من النتائج من خلال تناولها لموضوع مستوى الوعي السيبراني في الوسط الجامعي وعلاقته بالجريمة الإلكترونية، بما في ذلك تعريف القارئ بما يلي:

أ- معرفة وجهة نظر طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة حول الوعي السيبراني والجريمة الإلكترونية.

ب- تحديد درجة الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة.

ت- تحديد درجة الوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة.

ث- الكشف عن الفروق بين استجابة أفراد عينة الدراسة حول الوعي السيبراني والوعي بالجريمة الإلكترونية تعزى لمتغيرات (الجنس، السن، القسم، المستوى التعليمي).

ج- الكشف عن العلاقة بين الوعي السيبراني والوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية في جامعة خميس مليانة.

6.أسباب اختيار الموضوع

إن اختياري لموضوع "مستوى الوعي السيبراني في الوسط الجامعي وعلاقته بالجريمة الإلكترونية" كموضوع بحث يأتي نتيجة للأهمية البالغة التي يكتسيها هذا الموضوع في المجتمع الجزائري. فهو موضوع لم يسبق التطرق إليه بشكل مكثف، ومستمد من الواقع الاجتماعي، وله وزنه المعتبر فيه. وتظهر أهميته تلقائيًا من خلال المفاهيم المتضمنة فيه، وهما الوعي السيبراني والجريمة الإلكترونية. هذه الأهمية ترسخت في ذهن الباحث من خلال الاطلاع الدائم على الأخبار المتعلقة بظواهر وأشكال الجريمة

الإلكترونية المختلفة، مما خلق رغبة شخصية في التقرّب من هذه الظاهرة ومحاولة فهمها ومعرفة أسبابها. دوافع ذاتية وأخرى موضوعية تجعل الباحث مستعدًا للقيام بهذه الدراسة. ومن أهم الأسباب الدافعة لاختيار هذا الموضوع ما يلي:

الأسباب الذاتية:

- في إطار التحضير لنيل شهادة الدكتوراه، والعمل على التطرق إلى زاوية بحث جديدة في مجال دراسات الوعي السيبراني والجريمة الإلكترونية، بهدف الحد من الظاهرة الإجرامية التي تواجه الطلبة عند استخدام الإنترنت.
- الرغبة الشخصية في الكشف عن العلاقة بين مستوى الوعي السيبراني والوعي بالجريمة الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية بجامعة الجيلالي بونعامة بخميس مليانة.
- الرغبة في المساهمة في إيجاد حلول لمكافحة الجريمة الإلكترونية وتعزيز الوعي السيبراني بها، خاصة في الوسط الجامعي الجزائري.

الأسباب الموضوعية:

- نقص الدراسات التي تربط بين موضوع الوعي السيبراني والجريمة الإلكترونية في الجزائر.
- تزايد الجريمة الإلكترونية مع تزايد استخدام التكنولوجيا والإنترنت بشكل كبير في المجتمع الجزائري.
- التحول الرقمي الذي تشهده المؤسسات الجامعية الجزائرية يجعلها عرضة للهجمات الإلكترونية، ويُعتبر المورد البشري الحلقة الأضعف. لذا تم اختيار الموضوع للكشف عن مستوى وعيه السيبراني وتحديد برامج لتنميته وتجنب الجريمة الإلكترونية التي تهدده مستقبلاً.

7.مفاهيم الدراسة

تتضمن العلوم الاجتماعية العديد من المفاهيم، التي تحمل العديد من التعريفات المتنوعة والمتعددة، وهذا يمكن أن يؤدي إلى الارتباك وعدم الاستقرار في البحث الاجتماعي. لذا، من الضروري وضع تعاريف دقيقة ومحددة للمفاهيم في الدراسات العلمية. فيما يلي سنتناول مفاهيم دراستنا بالتفصيل:

1.7. مفهوم الوسط الجامعي

- **تعريف لغوي للجامعة:** تعني كلمة "جامعة" في الأصل اللاتيني "universitas" الجمعية التي تتولى ممارسة التعليم (الشيخ وبن زرقة، 2015، ص 11).
- **التعريف الاصطلاحي للجامعة:** فضاء يجمع طائفة من الباحثين لهم الحرية الكاملة لمباشرة البحث العلمي في أي مجال معرفي (مولاي، 2012، ص 191).
- كما تُعرف أيضًا على أنها مؤسسة علمية ثقافية تضم مجموعة من الطلبة والإطارات الكفوءة والأجهزة العلمية المتطورة، حيث تعمل على نشر العلم والمعرفة من خلال البحوث النظرية والميدانية.
- **التعريف الاصطلاحي للوسط الجامعي:** بيئة الأنسان الاجتماعية داخل الجامعة، وهو الحيز الذي يتحرك فيه الأفراد ويتفاعلون مع بعضهم، ويتضمن بيئات اجتماعية وتنظيمية ومادية (2003، ص 111).
- **التعريف الإجرائي للوسط الجامعي حسب دراسة الباحث:** العناصر الأساسية، المادية وغير المادية، المكونة للمؤسسة الجامعية، تتمثل في موردها البشري وكيانها التنظيمي ووظائفها (من تدريس وبحث علمي إلى الاقتصادية والسياسية). يجمع الوسط الجامعي بين التفاعل الواقعي والتفاعل الافتراضي نتيجة التطور التكنولوجي.

2.7. مفهوم الجريمة الإلكترونية

- **تعريف لغوي للجريمة:** "الجريمة" حسب ابن منظور هو التعدي، والجرم هو الذنب، والجمع أجرام وهو الجريمة (ابن منظور، 1971، ص 90).
- **تعريف اصطلاحي للجريمة الإلكترونية:** مجموعة من الأفعال والسلوكيات غير المشروعة التي يعاقب عليها القانون، ترتكب عبر أجهزة الكمبيوتر والشبكات الإلكترونية، وتشمل أنشطة مثل التجسس واختراق الأنظمة واستخدام المعلومات بشكل غير قانوني (Phillips et al.، 2022، ص 382).
- **التعريف الإجرائي للجريمة الإلكترونية حسب دراسة الباحث:** مرحلة تطورية للجريمة التقليدية، تعتمد على الإنترنت والتقنيات الإلكترونية، وتتجاوز الحدود الجغرافية والسياسية، وتشمل أنشطة مثل القرصنة والاحتيال الإلكتروني. تُعتبر جريمة في القوانين الجزائرية والدولية.

3.7. مفهوم الأمن السيبراني

- **التعريف اللغوي للأمن:** يُطلق مصطلح "الأمن" في اللغة العربية على حالة عدم الخوف والحفاظ والثقة، وطلب الحماية والسلام (جراية، 2014، ص 19).
- **التعريف الاصطلاحي للأمن السيبراني:** يُعرَّف الأمن السيبراني على أنه المجال الذي يهتم بحماية الأنظمة الإلكترونية من الهجمات سواء كانت داخلية أو خارجية على المؤسسات أو أجهزة وسائط الأفراد. يعتمد هذا التعريف على تقنيات حماية الشبكات والخوادم وأجهزة الكمبيوتر والمعلومات المتصلة بالإنترنت للدفاع ضد الهجمات غير المصرح بها وضمان الأمن ضد التهديدات السيبرانية (Von Solms & Van Niekerk، 2013، ص 99).
- **التعريف الإجرائي للأمن السيبراني حسب دراسة الباحث:** يُعرف الأمن السيبراني في السياق الجامعي على أنه مجموعة من الإجراءات التقنية والإدارية التي تتخذها المؤسسة لمنع أي اختراق غير مصرح به لنظامها الإلكتروني. هذه الإجراءات تتضمن العمليات والآليات التي تُنفذ لحماية البيانات الشخصية للأساتذة والطلاب وضمان سرية المعلومات، بالإضافة إلى حماية المعدات والتقنيات التي تستخدمها المؤسسة من الإتلاف.

4.7. مفهوم الوعي السيبراني

- **تعريف للوعي:** يُعرَّف الوعي في سياق علم الاجتماع على أنه القدرة على فهم الفرد لذاته وللبيئة المحيطة به بدرجات متفاوتة من الوضوح والتعقيد، وذلك من خلال فهم الوظائف العقلية والجسمية للفرد، بالإضافة إلى الوعي بالعالم الخارجي (غيث، 1989، ص 81).
- **التعريف الاصطلاحي للوعي السيبراني:** يُعرَّف الوعي السيبراني على أنه القدرة على التعرف على السلوكيات التي تحمي الأمان الإلكتروني وتواجه التهديدات الإلكترونية خلال استخدام الأجهزة الإلكترونية. يُسهم الوعي السيبراني في حفظ خصوصية وبيانات الفرد الشخصية والمعلومات الرقمية.
- **التعريف الإجرائي للوعي السيبراني حسب دراسة الباحث:** يُعرَّف الوعي السيبراني في السياق الجامعي على أنه مستوى الفهم الذي يمتلكه الطلبة حول أفضل ممارسات أمن المعلومات أثناء تفاعلهم عبر الإنترنت، مما يشمل التواصل عبر وسائل التواصل الاجتماعي والبريد الإلكتروني.

5.7. الطالب الجامعي

في دراسة الباحث، يُعرَّف الطالب الجامعي بأنه الشباب الذي تتراوح أعمارهم بين 17 و28 سنة وقد أكملوا مراحل التعليم الثلاث الأولى، وهي المراحل الابتدائية والمتوسطة والثانوية. يقومون بدراسة في جامعة جيلالي بونعامة، بكلية العلوم الإنسانية والاجتماعية، حيث يتابعون برامج اللسانس والماستر.

6.7. المستوى

في دراسة الباحث، يُعرَّف المستوى على أنه درجة الوعي السيبراني والوعي بالجريمة الإلكترونية. يتم تصنيفه إلى ثلاث مستويات: منخفض، متوسط، مرتفع، ويتم تحديدها من خلال اختبار الطالب باستخدام أداة بحثية.

8. الدراسات السابقة

تعتبر مرحلة استعراض الدراسات السابقة من الخطوات الأساسية والضرورية، في عملية البحث العلمي إنها تسهم في بناء الإطار النظري والأفكار، وتحديد الجوانب التي يجب أن يتخذها الباحث بعين الاعتبار بشكل دقيق وشامل في مشكلة البحث، ويمكن من خلالها التأكد من تغطية جميع الجوانب التي تؤثر على الدراسة بشكل كامل، وسوف يتم استعراض العديد من الدراسات العربية والأجنبية ذات الصلة بموضوع البحث وهي على النحو التالي:

1.8. الدراسة الأولى

دراسة مينال شاوهان وأربنا (2012) بعنوان:" الوقاية من جرائم الإنترنت: دراسة حول وعي جرائم الإنترنت في تريسيتي".

حيث هدفت الدراسة الحالية لتقديم نظرة عامة على جرائم الإنترنت، تدرس الوعي بين المشاركين المختلفين بشأن مسألة جرائم الإنترنت، وذلك لتؤكد على خطورة هذه المشكلة والحاجة الملحة للحد من تأثيرها في جميع أنحاء العالم.

الأسئلة الفرعية للدراسة:

1. هل توجد علاقة بين مهنة للمستجيب ومستوى الوعي بجرائم الإنترنت بينهم؟

منهج وأدوات الدراسة تم استخدام المنهج الوصفي واعتمد على الاستبيان كأداة بحثية.

العينة: العشوائية البسيطة مكونة من 100 فردة.

نتائج الدراسة: كشفت النتائج عن أهمية الوعي كأداة للحد من جرائم الإنترنت ومنعها، وبالتالي يتم التوصل إلى استنتاج أنه لا توجد علاقة بين مهنة المستجيب ومستوى الوعي، يعود ذلك إلى حقيقة أن هناك اعتقاداً شائعًا يؤدي إلى تقدير أدنى للتهديد الذي يمكن أن يواجه المجتمع ومن أهم النتائج هو الاستجابة المحتملة للسكان لتهديدات جرائم الإنترنت، وذلك استنادًا إلى مستوى الوعي لدى أفراد السكان بشأن جرائم الإنترنت، يمكن لبعض الأشخاص أن يتجاهلوا هذه المسألة ويعتبروها غير مهمة لأن الجريمة تحدث في العالم الافتراضي، الذي يعتبره البعض غير حقيقي، يرجع ذلك إلى أن هؤلاء الأفراد لديهم وصول أقل إلى العالم الافتراضي ولا يمتلكون معلومات أساسية حول التأثيرات المحتملة التي يمكن أن تنجم عن حدوث جريمة الإنترنت.

2.8. الدراسة الثانية

دراسة أنوبريت كور موخا (2017) بعنوان:"دراسة حول وعي بجرائم الإنترنت والأمان منطقة دلهي" .

هدفت الدراسة الحالية إلى زيادة الوعي بجرائم الإنترنت التي تحدث في عالمنا اليوم، وأيضًا للخلق وعي للأدراك الأمان السيبراني حيث تحاول هذه الدراسة تحليل الوعي بجرائم الإنترنت بين مستخدمي الإنترنت ذوي الفئات العمرية المختلفة، والمؤهلات التعليمية المختلفة.

الأسئلة الفرعية للدراسة:

1. هل توجد علاقة بين مستوى التعليم للمستجيب والوعي بجرائم الإنترنت بينهم؟

2. هل توجد علاقة بين مجموعات الأعمار المختلفة للمستجيب والوعي بجرائم الإنترنت بينهم؟

منهج وأدوات الدراسة تم استخدام المنهج الوصفي اعتمد على مقياس لايكرت بخمس نقاط مقسم الى أربعة أقسام، الأول للسمات الديمغرافية للأفراد العينة، وثاني حول تعامل مع استخدام الإنترنت لدى المشاركين، وثالثا حول مستوى الوعي بجرائم الإنترنت والأمان وأخيرا مستوى الوعي بالسلامة أثناء استخدام أجهزة الكمبيوتر الشخصية والإنترنت.

العينة: وبعد التأكد من دلالات الصدق والثبات، طبقت الأداة على 160 شخص مستخدمي الأنترانت في دلهي.

نتائج الدراسة: فقد توصل الدراسة إلى نتائج، أن هناك علاقة تتواجد بين فئات الأعمار والمؤهلات التعليمية للمستجيبين لذا، فمن واجب جميع مستخدمي الإنترنت أن يكونوا على دراية بجرائم الإنترنت والأمان وأيضًا مساعدة الآخرين من خلال زيادة الوعي بينهم.

3.8. الدراسة الثالثة

دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) بعنوان:" الجرائم الإلكترونية ومستوى الوعي بخطورتها: دراسة ميدانية على عينة من الشباب الجامعي الأردني".

هدفت هذه الدراسة إلى التعرف إلى الجرائم الإلكترونية، ومستوى الوعي بخطورتها من وجهة نظر الشباب الجامعي الأردني في جامعة البلقاء التطبيقية كلية الأميرة رحمة الجامعية والتعرف على عادات وأنماط استخدام الإنترنت لدى الشباب، وتحديد إن كان هناك فروق تعزى إلى الجنس، والتخصص، والسنة الدراسية، ولتحقيق هذه الأهداف انطلقت الباحثة من السؤال المركزي التالي: ما الجرائم الإلكترونية ومستوى الوعي بخطورتها لدي من الشباب الجامعي الأردني؟

الأسئلة الفرعية للدراسة:

1.ما مستوى تعرض الشباب الجامعي الأردني للجرائم الإلكترونية؟

2.ما عادات وأنماط استخدام الإنترنت لدى الشباب الجامعي الأردني؟

3.ما مستوى وعي الشباب الأردني بالجرائم الإلكترونية؟

منهج وأدوات الدراسة: فقد اعتمد الباحث على المنهج الوصفي، ومنهج المسح الاجتماعي والاستبيان مكون من (43) فقرة للإجابة على أسئلة الدراسة.

العينة: اعتمد على العينة العشوائية وقد بلغت 212 مفردة من الشباب الجامعي الأردني من جامعة البلقاء التطبيقية.

نتائج الدراسة: فقد توصل الدراسة إلى ان أن معدل تعرض الطلبة للجرائم الإلكترونية جاء بمستوى منخفض، كما بينت نتائج الدراسة أن 39.15% يقضون من ساعتين إلى أقل من أربع ساعات على الإنترنت، أما أكثر المواقع استخداماً فهو الفيس بوك بنسبة 49.06% و 43.40% يدخلون للمواقع بهدف الترفيه والتسلية، أما مستوى الوعي بالجرائم الإلكترونية فقد جاء مرتفعاً، وأوصت الدراسة بضرورة توعية الطلبة بأهمية استثمار وقتهم عند استخدام الإنترنت لتطوير مهاراتهم، تفعيل النشاطات

الرياضية، والثقافية، والترفيهية، لجذب الشباب للحد من الإدمان على مواقع التواصل الاجتماعي، عقد المحاضرات لتوعية بمخاطر الجرائم الإلكترونية.

4.8. الدراسة الرابعة

دراسة نهي مصطفي كمال أبو كريشه (2022) بعنوان:"الوعي المعلوماتي والجريمة الإلكترونية".

هدفت هذه الدراسة إلى الى تسليط الضوء على العلاقة بين الوعي المعلوماتي والجريمة الإلكترونية، والتعرف على رؤية المبحوثين للوعي المعلوماتي، والجريمة الإلكترونية ودور شبكات التوصل الاجتماعية في تنمية الوعي المعلوماتي ومدي تعرضهم للجريمة الإلكترونية، وتعرف على كيفية تنمية الوعي المعلوماتي، ولتحقيق هذه الأهداف انطلقت الباحثة من السؤال المركزي التالي: هل للوعي المعلوماتي لدي مستخدمي مواقع التواصل الاجتماعية دور في الوقاية من عدم التعرض للجريمة الإلكترونية ومجابهتها؟

الأسئلة الفرعية للدراسة:

1.ما رؤية المبحوثين لكل من الوعي المعلوماتي والجريمة الإلكترونية؟

2.ما مدى امتلك مستخدمي مواقع التواصل الاجتماعي لوعى المعلوماتي؟

3.هل أثرت مواقع التوصل نفسها على وعى مستخدميها وجعلتهم أكثر وعيا ودراية بالجريمة الإلكترونية وكيفية تفاديها؟

منهج وأدوات الدراسة: فقد اعتمد الباحث على المنهج الوصفي، والاستبيان الإلكتروني للإجابة على أسئلة الدراسة.

العينة: اعتمد على العينة العشوائية وقد بلغت 268 مفردة من مستخدمي شبكات التواصل الاجتماعي.

نتائج الدراسة: فقد توصل الدراسة إلى، ان الفيسبوك أكثر وسائل التواصل الاجتماعي استخداما وشيوعا، كما ساهمت شبكات التواصل الاجتماعي في زيادة معدل الجريمة الإلكترونية، وصعوبة ملاحقتها وكذلك فهنالك علاقة إيجابية بين الوعي المعلوماتي وبين الوقوع في الجريمة الإلكترونية وقد بين الدراسة ضعف مستوي الوعي المعلوماتي.

5.8. الدراسة الخامسة

دراسة حمد بن حمود السواط وآخرون (2020) بعنوان: " العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف".

هدفت هذه الدراسة إلى معرفة درجة الوعي بالأمن السيبراني وعلاقته بتوفر القيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية، والمتوسطة بمدينة الطائف وإلى دراسة العلاقة بين الوعي بالأمن السيبراني والقيم لديهم، وللكشف عن إمكانية التنبؤ بهذه القيم من خلال المعرفة بالأمن السيبراني، وأخيراً للكشف عن الفروق بين استجابة أفراد عينة الدراسة حول الوعي بالأمن السيبراني والقيم تبعاً لمتغيرات (الجنس، نوع المدرسة، المرحلة الدراسية، الحالة الاقتصادية للأسرة) ، ولتحقيق هذه الأهداف انطلقت الباحثة من السؤال المركزي التالي: ما لعلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدنية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف؟

الأسئلة الفرعية للدراسة:

1.ما درجة الوعي بالأمن السيبراني لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف؟

2.ما درجة توفر القيم الوطنية والأخلاقية والدنية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف؟

3.هل يمكن التنبؤ بالقيم الوطنية والأخلاقية والدنية من خلال توفر الوعي بالأمن السيبراني؟

4.هل توجد فروق ذات دلالة إحصائية بين متوسطات استجابة أفراد عيبة الدراسة حول الوعي بالأمن السيبراني والقيم تعزي لمتغيرات (الجنس، نوع المدرسة، المرحلة الدراسية، الحالة الاقتصادية للأسرة)؟

منهج وأدوات الدراسة: فقد اعتمد الباحث على المنهج الوصفي الارتباطي، لدراسة العلاقة بين الوعي بالأمن السيبراني وبعض القيم لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف والاعتماد على المقياس للإجابة على أسئلة الدراسة.

العينة: اعتمد على العينة العشوائية وقد بلغت (346) تلميذاً وتلميذة من المرحلتين الابتدائية (105 تلميذاً وتلميذة) والمتوسطة (241 تلميذاً وتلميذة)، داخل المدارس الحكومية (160 تلميذاً وتلميذة) ومدارس اللغات (186 تلميذاً وتلميذة)، بمدينة الطائف، وكان منهم (143) من الإناث، و(203) من الذكور، وقد أعد الباحثون مقياسي الوعي بالأمن السيبراني والقيم (الوطنية والأخلاقية والدينية).

نتائج الدراسة: فقد توصل الدراسة إلى نتائج أن درجة الوعي بالأمن السيبراني لدى التلاميذ مرتفعة بدرجة كبيرة جداً في مجال التعامل الآمن مع خدمات تصفح الإنترنت لدى تلاميذ المرحلتين الابتدائية والمتوسطة، بمدينة الطائف كما أن القيم الوطنية والأخلاقية والدينية متوفرة لديهم بدرجة عالية جداً، ووجدت علاقة قوية بين الوعي بالأمن السيبراني والقيم لدى أفراد العينة، واتضح إمكانية التنبؤ بالقيم الوطنية والأخلاقية والدينية من خلال الوعي بالأمن السيبراني، وقد وجدت فروق في معرفة التلاميذ بالأمن السيبراني، والقيم تعزى لمتغير المرحلة الدراسية ولصالح أفراد المرحلة الابتدائية، وكذلك في متغير دخل الأسرة ولصالح الدخل العالي، في حين لم توجد فروق ذات دلالة إحصائية في متغير الجنس (ذكر/ أنثى) ونوع المدرسة (حكومية/ لغات).

6.8. الدراسة السادسة

دراسة ايمان عبد الفتاح عبابنه (2022) بعنوان: " درجة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني من وجهة نظرهن وعلاقته ببعض المتغيرات" .

وهدفت هذه الدراسة إلى، تحديد درجة الوعي لدى معلمات اللغة العربية في المدارس الثانوية للإناث في الأردن بشأن أمان السيبراني من وجهة نظرهن، وعلاقته بالمتغيرات المؤهل العلمي وخبرة التدريس، والمنطقة الجغرافية ولتحقيق هذه الأهداف انطلقت الباحثة من السؤال المركزي التالي: ما درجة الوعي بالأمن السيبراني معلمات اللغة العربية للمرحلة الثانوية في الأردن؟

الأسئلة الفرعية للدراسة:

1.ما درجة الوعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني؟

2.هل توجد فروق ذات دلالة إحصائية عند مستوي (α= 0.05) في درجة الوعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني تعزيا لمتغيرات المؤهل العلمي، وخبرة التدريس، والمنطقة الجغرافية؟

منهج وأدوات الدراسة: فقد اعتمد الباحث على المنهج الوصفي، تم إعداد استبانة تحتوي على (30) فقرة.

العينة: اعتمد على واشتملت عينة الدراسة على (330) معلمة، تم اختيارهن بطريقة عشوائية متنوعة من معلمات اللغة العربية في المدارس الثانوية في الأردن في ثلاث مناطق جغرافية (الجنوب والوسط والشمال)، في الفصل الدراسي الأول من العام الدراسي 2022/2021.

نتائج الدراسة: فقد توصل الدراسة إلى نتائج كانت درجة الوعي على مستوى عال، وبالإضافة إلى ذلك، كانت هناك فروق معنوية على مستوى ($\alpha = 0.05$) في تقديرات عينة الدراسة نتيجة الأهلية الأكاديمية، وصالحة لصالح الدراسات العليا علاوة على ذلك، لم تظهر فروق على مستوى ($\alpha = 0.05$) في تقديراتهن نتيجة خبرة التدريس والمنطقة الجغرافية.

7.8. الدراسة السابعة

دراسة عبد الله بن حجاب القحطاني (2022) بعنوان: " درجة الوعي بالأمن السيبراني ذوي الإعاقة البصرية في المملكة العربية السعودية من وجهة نظرهم".

هدفت الدراسة الحالية الى التعرف على درجة الوعي بالأمن السيبراني لدى عينة من الأشخاص ذوي الإعاقة البصرية في المملكة العربية السعودية من وجهة نظرهم، ولتحقيق هذه الأهداف انطلقت الباحثة من السؤال المركزي التالي: ما درجة وعي الأشخاص ذوي الإعاقة البصرية في المملكة العربية السعودية بالأمن السيبراني من وجهة نظرهم؟

الأسئلة الفرعية للدراسة:

1.ما درجة وعي الأشخاص ذوي الإعاقة البصرية في المملكة العربية السعودية بمفاهيم وتطبيقات وسبل التعزيز للأمن السيبراني من وجهة نظرهم؟

2.هل توجد فروق ذات دلالة إحصائية عند مستوي ($\alpha= 0.05$) في درجة وعي الأشخاص ذوي الإعاقة البصرية بالأمن السيبراني تعزي لمتغير الجنس؟

3.هل توجد فروق ذات دلالة إحصائية عند مستوي ($\alpha= 0.05$) في درجة وعي الأشخاص ذوي الإعاقة البصرية بالأمن السيبراني تعزي لمتغير التدريب؟

4.هل توجد فروق ذات دلالة إحصائية عند مستوي ($\alpha= 0.05$) في درجة وعي الأشخاص ذوي الإعاقة البصرية بالأمن السيبراني تعزي لمتغير مستوي التعليم؟

منهج وأدوات الدراسة: تم استخدام المنهج الوصفي اعتمد على استبانة تكونت في صورتها النهائية من **جز أين الأول:** تضمن البيانات الشخصية للمشاركين، والثاني تضمن فقرات الاستبيان وعددها 30 فقرة موزعة على ثلاثة ابعاد هي: الوعي بمفاهيم الأمن السيبراني وتكون منم 10 فقرات، الوعي بتطبيقات الأمن السيبراني وتكون من 13 فقرة والبعد الثالث سبل تعزيز الوعي بالأمن السيبراني وتكون من 7 فقرات.

العينة: وبعد التأكد من دلالات الصدق والثبات طبقت الاداة الأداة على 56 شخص من ذوي الإعاقة البصرية.

نتائج الدراسة: فقد توصل الدراسة إلى نتائج لي ان الدرجة الكلية بالوعي بالأمن السيبراني متوسطة وكانت متوسطة، أيضا على البعد الأول ومرتفعة على البعدين الثاني والثالث كما اشارت النتائج، الى عدم وجود فرق دال احصائيا في درجة الوعي بالأمن السيبراني تعزى الى متغير الجنس والتعليم، بينما كان هناك فرق دال احصائيا حسب متغير التدريب يعود الى الأشخاص الذين حصلوا على تدريب على الامن السيبراني، وأخيرا فقد اوصت الدراسة بضرورة الاهتمام بالأمن السيبراني للأشخاص ذوي الإعاقة عموما وذوي الإعاقة البصرية بشكل خاص.

8.8. التعقيب على الدارسات السابقة:

بناء على العرض السابق للأهم الدراسات المرتبطة بالجريمة الإلكترونية، والوعي بها يحاول الباحث تحديد، ما اتفقت فيه الدراسات السابقة مع موضوع الدراسة الخاصة بي من حيث الموضوع والأهداف ونقاط التداخل والاختلاف وعرض، ما أغفلته من قضايا في تناولها للموضوع الدراسة مع توضيح أوجه الاستفادة في الدراسة الراهنة:

أ. من حيث الموضوع والأهداف:

انطلاقا من الدارسات السابقة، لقد توفقت العديد من الدراسة السابقة بالمتغيرات الأساسية لموضوع بحثنا الذي يدرس مستوي الوعي السيبراني في الوسط الجامعي وعلاقته بالجريمة الإلكترونية، فهنالك العديد من الدراسات التي اهتمت بالجريمة الإلكترونية وهي دراسة كل من مينال شاوهان وأربنا (2012) وأوبريت كور موخا (2017) ودراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) ودراسة نهي مصطفي كمال أبو كريشه (2022).

أضافة الى، العديد من الدراسة التي اهتمت بالأمن السيبراني والوعي به ومن بينها دراسة حمد بن حمود السواط وآخرون (2020) ودراسة ايمان عبد الفتاح عبابنه (2022) وعبد الله بن حجاب القحطاني (2022).

أما بنسبة الأهداف هنالك العديد من الدراسات التي تشاركت فأهداف درستنا الحالية ومن بينها دراسة مينال شاوهان وأربنا (2012) التي كانت حول " الوقاية من جرائم الإنترنت: دراسة حول وعي جرائم الإنترنت في تريسيتي"، ودراسة أنوبريت كور موخا (2017) التي كانت حول وعي بجرائم الإنترنت، والأمان بمنطقة دلهي و دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) التي كانت حول " الجرائم الإلكترونية ومستوى الوعي بخطورتها: دراسة ميدانية على عينة من الشباب الجامعي الأردني وفي الأخير دراسة عبد الله بن حجاب القحطاني (2022) " درجة الوعي بالأمن السيبراني ذوي الإعاقة البصرية في المملكة العربية السعودية من وجهة نظرهم".

ب. من حيث الأساليب المنهجية:

هنالك العديد من الدارسات التي اعتمدت على نفس المنهج المعتمد في دراستنا الذي هو المنهج الوصفي الارتباطي، لكن كانت اختلافات من حيث المتغير الثاني لدراستهم ومن بين هذي دراسات مثل دراسة أنوبريت كور موخا (2017) التي كانت حول وعي بجرائم الإنترنت وعلاقته بالأمان، ودراسة حمد بن حمود السواط وآخرون (2020) التي درست العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية، وقد اعتمدت هذه الدراسات على نفس الأداة البحثية والمنهج اختلقت في جانب متغيرات المدروسة ومجتمع الدراسة.

ج. الاستفادة من الدراسات السابقة

كان للدارسات السابقة دور كبير في العديد من المجالات والجوانب المعرفية والمنهجية والإجرائية للأطروحة وتوضيحها، وذالك كما يلي:

1.اختيار موضوع وتحديد اشكالية الدراسة وصياغة تساؤلاتها وفرضياتها البحثية، فبعد الاطلاع على مجموعة من الدراسات العلمية، التي تناولت متغيري الوعي السيبراني والجريمة الإلكترونية قررنا القيام بهذه الدراسة لفهم، وتحليل طبيعة العلاقة القائمة بينهما.

2.التعرف على مختلف المصادر والمراجع، التي اعتمدتها الدراسات السابقة والتي ساعدتنا في توفير الوقت، والجهد في عملية المسح المكتبي، للإعداد وبناء الجانب النظري للأطروحة بمختلف فصوله.

3.الاطلاع على منهجية الدراسات السابقة في جانبها النظرية والميدانية، مما سهل أمامنا لبناء الأطار النظري للموضوع دراستنا، وتحديد المجال المكاني لدراسة وتصميم الأداة البحثية وانتقاء أدوات جمع البيانات ومعرفة الخطوات العلمية، والإحصائية للتأكد من صدق وثبات أداتي الدراسة.

4.كما مكنتنا الدراسات السابقة من إجراء مناقشة للنتائج التي توصلنا إليها، من خلال مقارنتها مع نتائج هذه الدراسات.

9.مقاربات نظرية للموضوع

ان الجريمة الإلكترونية من الظواهر التي أصبحت ملاحظة في الواقع الافتراضي باعتبارها مأثرة على الأفراد والمؤسسات وخاص الوسط الجامعي، ومكوناته حيث تشكل عليهم تهديدا في مسار حياتهم بحكم اختلافها عن الجريمة التقليدية باعتبار أن كل فرد من الوسط الجامعي مهما كان طالب او أستاذ او عاملين متفاعلين ومتصلين دائما بالأنترانت، لهذا فهم دائما مستهدفين من طرف مجرمين الافتراضيين، وقد تعددت وجهات نظر العلماء والبحثين في مجال العلوم الاجتماعية، والجريمة حول الجريمة الإلكترونية في الوسط الجامعي فمنهم من يعتبره سلوك مكتسب نتيجة التفاعل مع الأخرين، ومنه من يراه سلوك مكبوت يمارس في الواقع الافتراضي، وتحقيق للأهداف دراستنا وتوضيحها تم اللجوء الى النظريات المفسرة للجريمة الإلكترونية وتتوافق مع موضوعنا.

1.9. نظرية الارتباط التفاضلي لسندرلاند

تعتبر نظرية الارتباط التفاضلي لسندرلاند من النظريات القديمة التي استخدمت في تفسير الجريمة الإلكترونية، وهي نموذج لنظريات التعلم الاجتماعي وتم تقديم هذه النظرية سنة 1939 وتفترض أن الإجرام، في جزء كبير منه، يمثل عملية التنشئة الاجتماعية اختصارا لعبارة "الارتباط التفاضلي مع الأنماط السلوكية الإجرامية والمناهضة للإجرام النظرية يعمم أن البشر يتعلمون المشاركة في الانحراف من التعرض للسلوك الإجرامي والمواقف من خلال الارتباط مع أقران مقربين وموثوق بهم، مزيد من الاستكشاف في هذه النظرية يكشف فكرة أن تعلم السلوك الإجرامي هي عملية مشابهة لتعلم أي نوع آخر من السلوك (الدوسري، 2021).

حيث جاءت هذه النظرية بمجموعة من الأفكار التي من خلالها يمكننا تفسير جريمة الإلكترونية حيث أن فكرتها الأساسية التي تقوم عليها تري أن تعلم السلوك الإجرامي هو نتيجة لتفاعل مع الأخرين داخل مجموعة من الأشخاص تجمعهم علاقة ارتباطية من خلال التأثير وتأثر فيما بينهم.

أ-تعلم السلوك الإجرامي في الواقع الافتراضي بتضمن تعلم التقنيات ارتكاب الجريمة بإضافة الى توجيه الدوافع نحو الأجرام والتبريرات والمواقف، من خلال تعريف بالنصوص القانونية المواتية وغير الملائمة بنسبة إليهم.

ب-علاوة على هذا، يصبح الشخص مجرما عند عملية التواصل والتفاعل مع المنحرفين التي تدفعه بانتهاك القوانين الوضعية، كما توجد فروق في العلاقة بين المجرمين من حيث التردد والمدة والأولوية والشدة التي تحدد صلة بينهم.

ت-فعملية تعلم السلوك الإجرامي له علاقة بالأنماط الجنائية وجميع الأليات التي تعتمد في الجريمة يستخدمها المجرم لتعبير عن الاحتياجات والقيم العامة واستخدمت أفكار هذه النظرية في تفسير السلوكيات الإجرامية الملاحظة في الأنترانت.

2.9.نظرية الانتقال الى الفضاء

تعتبر نظرية الانتقال الى الفضاء من النظريات الحديثة المفسرة للجريمة الإلكترونية حيث تم نشرها كفصل في كتاب "جرائم الإنترنت" الذي تم تأليفه كل من فرانك شماليجر ومايكل بيتارو وبرنتيس هول، وفي ضوء الحاجة الى نظرية منفصلة لتفسير أسباب الجريمة الإلكترونية وخاصة ان التفسير النظري العام الذي يرتكز على النظريات الكلاسيكية، في تفسير الجريمة الإلكترونية غير كاف كتفسير شامل لظاهرة الجريمة السيبرانية وقد جاءت هذه النظرية لتفسير لطبيعة السلوك الأشخاص المطبق في الواقع الافتراضي، وغير مطبق في الواقع المادي ومرحلة انتقال بحسب النظرية هي عملية التفاعل من الواقع الى الوقع الافتراضي من خلال الاعتماد على الوسائط الإلكترونية مرتبطة بالأنترانت حيث تتمحور فكرتها الرئيسة أن الأشخاص عند انتقاله الى الواقع الافتراضي يتصرفون بشكل مختلف حيث جاءت بمجموعة من الافتراضات مفادها(Jaishankar, 2007, p. 7) :

أ-أن الأشخاص الذين يتم قمع سلوكهم الإجرامي في الواقع المادي، بسبب موقعها وظروفها يكون كدافع لهم لممارسة الجرمية في الواقع الافتراضي.

ب-كمأن مروتة الهوية الرقمية وإمكانية إخفائها وغياب الردع كلها عوامل تدفع بارتكاب الجريمة الإلكترونية في الواقع الافتراضي.

ت-علاوة على هذا، تري نظرية الانتقال الى الفضاء أن الأشخاص يمكنهم نقل السلوك من الواقع الاجتماعي ويمارسونه على واقع الافتراضي أو عكس ذلك من خلال أستراد سلوكيات إجرامية ممارسة في المواقع الافتراضية ويتم تطبيقها في الحياة الاجتماعية.

ث-كما تسهل البيئة الافتراضية الهروب من الردع القانوني بحكم غياب الأدلة التي تثبت أدانة المجرم الإلكتروني حيث المرونة التي تتميز بها البنية الافتراضية من المحتمل أن يتجمع فيها المجرمون وتحدون بحكم أنهم تجمعهم نفس الأهداف والغايات او من خلال الاتحاد في الواقع المادي وممارسة الجريمة في الواقع الافتراضية.

ج-كما تري أن الأشخاص الذين يعيشون في المجتمعات المنغلقة هم أكثر ممارسة للجرائم الأنترنت على عكس الأفراد الذين يعشون في المجتمعات المفتوحة

ومن خلال هذا يمكن القول إن نظرية انتقال الى الفضاء قد سايرت علم الأجرام من خلال تناول الظواهر الإجرامية في فضاء الإلكترونية، كمكان جديد لها والتي تستوجب نظريات حديثة تفسر نشطات الجريمة الجديدة.

3.9.نظرية النشاط الروتيني

تركز نظرية النشاط الروتيني كمنهجية لمنع الجريمة على العناصر الأساسية التي تشكل جريمة حيث توفر هذه النظرية إطارًا يمكن من خلاله منع الجريمة من خلال، تغيير واحد على الأقل من هذه العناصر (الجاني أو الهدف أو وجود ولي أمر قادر) ويعتبر رائد هذه النظرية كل من "ماركوس فيلسون" و" كوهين "سنة 1979م وقد نشأت في الولايات المتحدة الأمريكية لدراسة تطور الأوضاع الاجتماعية، ومنها الأوضاع الإجرامية في الولايات الأمريكية بعد الحرب العالمية الثانية، دف الوصول إلى نظرية النشاط الروتيني حيث انتقدت النظرية البنائية الوظيفية وقصورها في تفسير الجريمة، والجنوح في الولايات المتحدة الأمريكية عندما تحسنت الأوضاع الاجتماعية(John, 2021, p. 15) .

كمأن في تفسيرها للجريمة تركز على عناصر الثلاثة في ذلك:

أ-هدف يمكن الوصول إليه.

ب-عدم وجود أوصياء قادرين يمكن أن يتدخلوا.

ت-وجود مجرم متحمس، هدف يمكن الوصول إليه.

حيث تجمع هذه العناصر الثلاثة الأنشطة الروتينية التي تجمع بين الجاني والمجني عليه في الزمان والمكان، حيث يعتبر وجود الجاني مع هدف الأجرام، ومجني عليه يغيب عليه الرقابة ويعتبر بذلك هدف مناسب، ومن خلال هذه المكونات الثلاثة حسب نظرية النشاط الروتيني يكون احتمال لوقع الجريمة الإلكترونية على المتفاعلين مع الحياة الافتراضية.

الفصل الثاني:

الجريمة الإلكترونية والوسط الجامعي

II. الفصل الثاني: الجريمة الإلكترونية والوسط الجامعي

1 ماهية الجريمة الإلكترونية.

1.1 مفهوم الجريمة الإلكترونية

2.1 وسط الجريمة الإلكترونية

3.1 مكونات وسط الجريمة الإلكترونية

4.1 خصائص الجريمة الالكترونية:

5.1 أنواع الجريمة الإلكترونية

2 تقنيات الجريمة الإلكتروني

1.2 مفهوم تقنيات الاختراق الإلكتروني

2.2 أنواع تقنيات الاختراق الإلكتروني

3.2 المشكلات الناتجة عن تقنيات الاختراق الإلكترونية

4.2 أسباب الوقع ضحية للجريمة الإلكترونية

5.2 إستراتيجيات الوقاية من جرائم الإنترنت.

3 ماهية الوسط الجامعي

1.3 مفهوم الوسط الجامعي.

2.3 وظائف الوسط الجامعي.

3.3 مكونات الوسط الجامعي.

4.3 أهداف الوسط الجامعي

5.3 تدابير الحماية الوسط الجامعي من الجريمة الإلكترونية

تمهيد

تعتبر الجريمة الإلكترونية ظاهرة قديمة طورتها العولمة من خلال نقلها من الواقع المادي الى الواقع الافتراضي، فبرغم من أن للتقنيات التكنولوجيا كانت لها عديد من الأثار الأجابية على حياة البشر، من خلال تسهيل انتقال المعلومات بين الأفراد بسرعة فمن خلالها العالم أصبح قرية صغيرة، إلا أنها أنتجت عديد من عيوب حيث أصبحت المجتمعات في الآونة الأخيرة تعاني من ظاهرة إجرامية خطيرة مستجدة تعرف بالجريمة المعلوماتية، تنتهك الخصوصية الرقمية وبيانات للأفراد والمؤسسات، وتهدد بأمن واستقرار الدول، وهذا راجع لخاصية تجاوزها الحدود الإقليمية لها، كمأن أصبحت الجامعة الجزائرية ومكونات وسط الجامعي تحت تهديد الجريمة الإلكترونية نتيجة العملية التفاعلية، بين المؤسسة الجامعية والفضاء الإلكترونية في تحقيق أهدافها مما جعل بئتها الرقمية، ومكونها البشري ضحايا لعديد من الجرائم عدة، كالقرصنة الاحتيال، المواد الإباحية، تخريب الكمبيوتر، وقواعد المعلومات...الخ، فمن خلال هذا الفصل الذي يتناول الجريمة الإلكترونية والوسط الجامعي، يتم تعريف القارئ على ماهية الجريمة الإلكترونية من خلال تعريف الجريمة الإلكترونية ووسطها ومكونات هذا الوسط وأنواع الجرائم الإلكترونية وخصائصها

إضافة الى، تقنيات الجريمة الإلكتروني حيث، نقدم تعريف للتقنيات التي يستخدمها المجرمون في الجريمة الإلكترونية وأنواعها والمشكلات الناتجة، والأسباب التي تجعل الأفراد ضحايا للجريمة الإلكترونية ونحدد إستراتيجيات الوقاية من جرائم الإنترنت، وفي الأخير نتطرق الى الوسط الجامعي من حيث مفهومه، ومكوناته ووظائفه إضافة الى أهدافه وتدابير الحماية الوسط الجامعي من الجريمة الإلكترونية.

1.ماهية الجريمة الإلكترونية

1.1. مفهوم الجريمة الإلكترونية

شهد المجتمع المعاصر تطوراً سريعاً في العديد من جوانبه، وخاصة في مجال التكنولوجيا، مما جلب الكثير من وسائل الراحة في حياتنا مثل الحوسبة والإنترنت. وعلى الرغم من الجوانب الإيجابية لهذا التطور، إلا أنه تسبب أيضًا في ظهور مشكلات وزيادة حدة العديد من الظواهر التي تهدد استقرار البنية الاجتماعية، حيث أصبح من الصعب حلها والحد منها. على سبيل المثال، ظهرت أنواع جديدة من الجرائم؛ فإلى جانب الجرائم المعروفة في الوسط الاجتماعي مثل السرقة والاحتيال، أعطى التطور التكنولوجي شكلاً جديدًا لهذه الجرائم (بن مالك، **2019**، ص **102**).

في هذا السياق، من حيث المفهوم، أصبحت تُعرف هذه الجرائم بـ "الجرائم الإلكترونية"، وبرزت علاقة تفاعلية بين الظاهرة الإجرامية وتكنولوجيا المعلومات. فكلما استمرت هذه التكنولوجيا في التطور، تغيرت القضايا الجنائية، من حيث بروز مرتكبي هذا النوع من الجرائم، أي "المجرمين"، وازداد عدد الضحايا وتنوعهم. نظرًا لأن هذه التكنولوجيا توفر سهولة ومرونة في التنقل لمستخدميها، فقد أصبحت وسيلة للمجرمين لتحقيق أهدافهم غير المشروعة (المطيري وإدبيس، **2023**، ص **1249**).

ومع عولمة الظاهرة الإجرامية، التي تعني محو الحدود الدولية وجعل مراقبتها أكثر صعوبة، سواء من خلال الكشف أو المنع أو القبض على مرتكبي الجرائم عبر الإنترنت. أصبحت تكنولوجيا المعلومات والأجهزة الإلكترونية وغيرها من المنتجات عالية التقنية مثل الكمبيوترات والهواتف والإنترنت وجميع أنظمة المعلومات الأخرى، المطورة لمنفعة الإنسانية، عرضة للنشاط الإجرامي. على الرغم من أن "الجريمة الإلكترونية" أصبحت عبارة شائعة اليوم، إلا أنها من الصعب تعريفها بدقة. تم تطوير معظم التعاريف الموجودة بشكل تجريبي (**ÇAKIR** و**Ercan**، **2011**، ص **130**).

لذلك، عرف كل من **جوردون وفورد (2006)** الجرائم الإلكترونية على أنها: "أي جريمة يتم تسهيلها أو ارتكابها باستخدام جهاز كمبيوتر أو شبكة أو جهاز"، حيث قد يكون جهاز الكمبيوتر أو الجهاز هو عامل الجريمة، الميسر للجريمة، أو هدف الجريمة. ومن خلال هذا التعريف، يمكن اعتبار الجريمة الإلكترونية نشاطًا إجراميًا يُمارس بواسطة الإنترنت أو نظام الكمبيوتر أو تكنولوجيا الكمبيوتر (**Gordon & Ford**، **2006**، ص **15**).

من ناحية أخرى، هناك من يرون أن الجريمة الإلكترونية هي نتيجة لأنشطة سيبرانية للأفراد عبر مواقع الويب والشبكات الاجتماعية وتطبيقات الدردشة والمدونات والألعاب عبر الإنترنت والمراسلة والبريد الإلكتروني. إنها مشكلة أخلاقية تتجمع فيها العديد من الأسباب، وتنتج أشكالًا من التمييز والإساءة والترهيب والتهميش، مما يُبرز الجانب غير الأخلاقي للفرد. عادةً ما يكون لدى الكارهين نية إيذاء المجموعة أو الشخص الآخر، مما يعرضهم لمزيد من الهجمات، بما في ذلك الهجمات الجسدية في العالم "غير الافتراضي".

وبالإضافة إلى ذلك، فإننا نسمح بإمكانية مشاركة الأشخاص عن غير قصد على الإنترنت، من خلال التواصل بلا مبالاة بطرق قد تتضمن تعبيرات مسيئة بطبيعتها وتعرض الآخرين كأهداف قابلة لمزيد من الهجمات. يمكن متابعة "Cyberhat" من قبل أفراد. بالإضافة إلى ذلك، فإن السيبرانية لها طابع حركي، مثل ظاهرة الكراهية العلنية. فهي تظهر هدف المرء في الوقت نفسه، مما يجذب انتباه الكارهين الآخرين

ويشجعهم على أن يصبحوا نشطين ضد نفس الأهداف أو أهداف مشابهة. يمكن للنشاط الجماعي المتمثل في الكراهية أن يزيد من قوة الكراهية وحزم الكارهين في إلحاق الضرر بأهدافهم إلى حد كبير. السيبرانية هي أيضًا ظاهرة تسمم متبادل (**Dilek et al., 2015**، ص **23**).

من خلال هذا التحليل، يمكن إعطاء تعريف إجرائي للجريمة الإلكترونية. إذ تعتبر الجريمة الإلكترونية مرحلة تطورية للجريمة التقليدية من حيث أدواتها والمسرح وممارساتها. لم تعد تقتصر على الحدود السياسية والجغرافية، بل عرفت تنظيمًا واسعًا من حيث تشكل المجرمين وتواصلهم، بحكم العولمة التي كانت سببًا بارزًا في تغيرها. أصبح المجرم يعتمد على الإنترنت والوسائط الإلكترونية مثل الحاسوب والهاتف والألواح الإلكترونية كتقنيات ذات منفعة إنسانية. وقد أدى الاستخدام السيء لهذه التقنيات من قبل المنحرفين الإلكترونيين إلى ظهور الجريمة الإلكترونية وتطور أنواع هذه الجريمة. حيث حافظت الجريمة على طابعها التقليدي مثل (السرقة، العنف الرمزي)، لكن تنوعت أشكال ممارستها مثل (السرقة الإلكترونية، العنف الرمزي بالتعليقات العنصرية، وما إلى ذلك).

2.1.مفهوم وسط الجريمة الإلكترونية

يُعتبر مفهوم السوق من المفاهيم غير المألوفة في حقل علم الاجتماع، ولكنه برز في دراسات الاقتصاديين الأمريكيين غاري بيكر (Gary Becker) وإسحاق إيرليش (Isaac Ehrlich)، اللذين استخدما مفهوم سوق الجريمة في أعمالهما العلمية. يعتمد نموذج السوق للجريمة على خمس افتراضات رئيسية تتعلق بتكلفة الجريمة، والتأثيرات الاقتصادية للجريمة على المجتمع والأفراد، وعوامل تحديد الطلب والعرض للجرائم.

أولاً، يرى الباحثان أن سوق الجريمة هو تفاعل بين الجناة، الذين يعتبرون مقدمي الخدمات غير القانونية، والضحايا المحتملين، وهم مشترون لهذه السلع. يُعتبر القانون مجموعة من القواعد التي تضبط وتحسن السلوك في البيئة الافتراضية.

ثانياً، يُشكل الجناة المحتملون توقعات حول الفرص النسبية للخدمات القانونية وغير القانونية المقدمة عبر الإنترنت، بما في ذلك شدة العقوبة واليقين، بناءً على المعلومات المتاحة. وبالتالي، يربطون التوقعات الذاتية بالفرص الموضوعية.

علاوة على ذلك، يفضل الجناة المحتملون بين الوقوع في الجريمة أو تفضيل السلامة الجنائية خلال أي عملية تخالف القوانين الوضعية. بحكم أن الجريمة عامل خارجي مزعزع للاستقرار، فإن تطبيق

القانون يحقق المصلحة العامة ويحمي الأشخاص المتفاعلين في الواقع الافتراضي. إضافةً إلى ذلك، تضمن الأحكام المجمعة لسلوك جميع الأطراف ذات العلاقة توازنًا واضحًا، مما يؤدي إلى توازن في نموذج الجريمة.

من خلال أفكار نموذج سوق الجريمة، يتضح أن تفاعل الضحايا المحتملين وتعاقدهم في المعاملات غير المشروعة التي يقدمها الجناة لا يتم بالضرورة في الأماكن المادية (العالم الواقعي)، بل يتم التعاقد أيضًا في العالم الافتراضي. يمكن تنسيق السلوك بين الموردين والمطالبين وجعله متسقًا بشكل متبادل. في هذا السياق، يقول غاري بيكر (1974): "يتحقق التوازن فقط من خلال التفاعل بين الجناة وتنفيذ القانون في الواقع". فكلما زاد الردع من طرف المؤسسات المعنية بمحاربة الجريمة الإلكترونية لكل من يمارس نوعًا من أنواع الجرائم باستخدام الحاسب وشبكة الإنترنت في العالم الواقعي، كلما زاد الاستقرار في البيئة الافتراضية (**Becker & Landes، 1974، ص 20**).

وبالنظر إلى ما تقدم، يرى إيرليش (1996) أن سوق الجرائم الإلكترونية هو "محيط تفاعل بين فئة الأفراد غير المجرمين والضامنين للقانون الذين يتدخلون في هذا السوق" (**Ehrlich، 1996، ص 46**). بناءً على ذلك، يمكن تعريف سوق الجريمة الإلكترونية إجرائيًا بأنه المحيط الذي يتفاعل فيه كل من الجاني والضحية والضامنين من القانونيين بصفتهم المراقبين. يجب أن تتوفر في الأفراد خصائص محددة، وإذا غابت هذه الخصائص، تقع الجريمة.

يُعتبر السوق المحيط الافتراضي الذي يجمع الجناة والضحايا والضامنين، حيث يُعتبر الضحية العنصر الأساسي، ويكون هدفًا من طرف الجاني ومحميًا من طرف الضامنين من القانونيين. بحكم أن السوق الإلكتروني يقدم العديد من الخدمات للضحية مثل التجارة والتحويل المالي والشراء عبر الإنترنت، تستوجب هذه التعاملات الوعي السيبراني من حيث وسائل الحماية التي يعتمد عليها في حماية بطاقته وحسابه المصرفي، بالإضافة إلى الأشخاص الذين يتعامل معهم والمواقع الإلكترونية التي يقتني منها أغراضه، والتي يجب أن تكون موثوقة. إذا تقيد الضحية بهذه الشروط، تقل نسبة وقوعه ضحية للجريمة.

في النهاية، تحدث الجريمة الإلكترونية إذا قدم الجاني خدمة غير قانونية للضحية. قد تكون هذه الخدمة عبارة عن سلعة وهمية على موقع إلكتروني أو عمولة مالية قام الضحية بتحويلها دون أن يحصل على الخدمة. يؤدي غياب الردع القانوني للجاني في الواقع المادي إلى اختلال التوازن بين الفاعلين في الواقع

الافتراضي، مما يزيد من عدد المجرمين الذين يستغلون الثغرات القانونية، ويؤدي إلى سقوط العديد من الضحايا في الجرائم الإلكترونية.

3.1. مكونات وسط الجريمة الإلكترونية

الجرائم الإلكترونية، مثل غيرها من الجرائم التقليدية، تشمل طرفين أساسيين، هما الجاني والمجني عليه، بالإضافة إلى هياكل المراقبة المكلفة بالردع والحماية. ومع ذلك، فإن أطراف الجريمة المعلوماتية تختلف عن أطراف باقي الجرائم الأخرى (المقصودي & علي، **2017**، ص**108**).

1.3.1. مجرم الإنترنت

مفهوم مجرم الإنترنت واسع، ويشمل جميع الأفراد الذين يُحتمل أن يرتكبوا جرائم على نظام الكمبيوتر أو عبر وسائط متصلة بشبكة الإنترنت. تتنوع أشكال الجرائم الإلكترونية التي يمارسها هؤلاء الأفراد، حيث يُعتبر سلوكهم ناتجًا عن سوء استخدام الوسائط الإلكترونية. تشمل هذه الجرائم خروقات البيانات والنظام وأجهزة الكمبيوتر (القرصنة)، تزوير بيانات الكمبيوتر، الاحتيال باستخدام أجهزة الكمبيوتر، نشر مواد إباحية تشمل الأطفال، وانتهاكات حقوق النشر مثل نشر المحتوى المقرصن (**Przyswa, 2010**، ص**12**).

حتى الآن، لم تتضح الصورة بالكامل في تحديد صفات مجرمي الإنترنت وشرح سماتهم النفسية ودوافعهم، نظرًا لقلة الدراسات الخاصة بهذه الظاهرة وصعوبة فهم مداها الحقيقي، بالإضافة إلى التطورات السريعة في مجال الكمبيوتر والإنترنت. رغم ذلك، يمكن تصنيف مجرمي الإنترنت حسب المنظور النفسي إلى فئتين أساسيتين:

- **فئة المتطفلين:** يرتكبون الجرائم بدافع التحدي والإبداع، وينصبون أنفسهم كأوصياء على أمن الحاسوب في المؤسسات المختلفة وحمايتها.
- **فئة المحترفين:** يمتازون بالخبرة والفهم الواسع للمهارات التقنية، ويتميزون بالتخطيط والتنظيم في أنشطتهم الإجرامية. يهدفون إلى تحقيق مكاسب مادية أو تحقيق أغراض سياسية أو فلسفية (الرومي، **2003**، ص**12**).

2.3.1. ضحايا الجريمة الإلكترونية

ضحايا الجريمة الإلكترونية تشمل أفراد الأسرة، الشركات، والحكومات الذين يستخدمون الإنترنت أو الكمبيوتر في حياتهم اليومية لأغراض مختلفة. يتعرض هؤلاء لنوع من أنواع الجرائم السيبرانية من قبل مجرمي الإنترنت، مما يجعلهم ضحايا محتملين لأسباب متنوعة (**Salu, 2005**، ص**161**).

3.3.1. هياكل المراقبة

تشمل هياكل المراقبة المؤسسات التنظيمية التي تهدف إلى منع إساءة استخدام الوسائط الإلكترونية وضمان تنفيذ الخدمات عبر الواقع السيبراني. تشمل هذه المؤسسات الأمنية التقليدية مثل الشرطة والدرك. إلا أن هذا النوع من الأمن التقليدي أظهر عدم قدرته على ضبط هذا النوع الجديد من الجرائم بسبب غياب مسرح الجريمة عن الواقع المادي وغياب الأدلة الجنائية التقليدية. لذا، يتم تطوير هياكل المراقبة بالاعتماد على الأمن السيبراني الذي يهتم بالجرائم التي تُرتكب في الواقع الافتراضي وعلى أنظمة الكمبيوتر (**Wall, 2007**، ص**185**).

من خلال هذا التحليل لمكونات وسط الجريمة الإلكترونية، يمكن أن نرى كيف أن التفاعل بين المجرم والضحية في البيئة السيبرانية يختلف عن التفاعل في الجرائم التقليدية. كما أن تطوير هياكل المراقبة لتتواكب مع هذا النوع من الجرائم يُعدّ أمرًا بالغ الأهمية لضمان أمن واستقرار الفضاء السيبراني.

وسط الجريمة الإلكترونية هو تركيبة تشمل ثلاثة فاعلين أساسيين:

- **المجرم الإلكتروني:** يتميز بسلوك انحرافي يمارسه عبر الوسائط الإلكترونية المتصلة بالإنترنت.
- **الضحية:** هو المتضرر من فعل المجرم، والذي يصبح ضحية بسبب عدم وعيه السيبراني وغياب أساليب الحماية.
- **هيكل المراقبة:** هو المسؤول عن توازن السوق الإلكتروني من خلال الردع القانوني ومراقبة التفاعل، وذلك عبر تطوير وسائل الأمن التقليدي واعتماد وسائل الأمن السيبراني.

من خلال هذا النموذج المتكامل، يمكن فهم ديناميكية الجريمة الإلكترونية وكيفية التعامل معها من خلال التعاون بين جميع الأطراف المعنية لضمان أمن واستقرار الفضاء السيبراني.

4.1. خصائص الجريمة الالكترونية:

تتميز الجريمة الإلكترونية بمجموعة من الخصائص التي تستمدها من طبيعة البيئة التي تُمارس فيها والأدوات التي تُرتكب بها، مما يجعلها مختلفة عن الجرائم التقليدية. من أبرز هذه الخصائص:

1. **أداة الارتكاب:** يُعتبر الحاسوب الآلي الأداة الرئيسية التي يستخدمها المجرم الإلكتروني للتسلل إلى شبكة الإنترنت وارتكاب جرائمه. يُشكل هذا الجهاز خاصية مميزة في عالم الجريمة الإلكترونية، حيث يُعتمد عليه كوسيلة وحيدة لتحقيق الأهداف الإجرامية (**Mohamed, 2016, p. 91**).

2. **موقع الارتكاب:** يُعتبر الإنترنت أو الشبكة العنكبوتية عنصرًا أساسيًا في الجرائم الإلكترونية، حيث يُستخدم كوسيلة للربط بين الأهداف المحتملة للهجمات الإلكترونية، مثل الشركات الصناعية والمصارف والهيئات الحكومية. ونظرًا لهذه المخاطر، تتخذ هذه الأهداف إجراءات أمنية إلكترونية لحماية نفسها من الهجمات الإلكترونية وتقليل حجم الخسائر المحتملة (بكوش & أمين, **2022**، ص**138**).

3. صعوبة الاكتشاف: تتميز الجريمة الإلكترونية بصعوبة اكتشافها. بشكل عام، لا يتم اكتشافها بسهولة، وإذا تم الكشف عنها، فإن ذلك يكون عادةً بالصدفة. يمكن القول إن نسبة اكتشاف الجريمة الإلكترونية قليلة جدًا مقارنةً بالجرائم التقليدية، وذلك لعدم وجود أي أثر خارجي مرئي لهذا النوع من الجرائم، وغالبًا ما تُرتكب الجريمة الإلكترونية خارج الدولة وفي قارات أخرى (**Alhemeiri et al., 2020, p. 770**).

4. عابرة للحدود: تُعد الجريمة الإلكترونية جريمة عابرة للحدود، فلا يتم ارتكابها داخل إقليم أو بلد واحد فقط. مع ظهور شبكات المعلومات التي لا تعرف حدودًا مرئية أو ملموسة، أصبحت إمكانية ربط عدد هائل من أجهزة الحاسوب عبر الشبكة العنكبوتية دون تقييد زمني أو مكاني متاحة. يمكن أن يكون المتهم في بلد والمجني عليه في بلد آخر، مما يُعقد جهود التحري والتنسيق الدولي لمكافحتها. تُعد الجريمة الإلكترونية صورة حقيقية لظاهرة العولمة، حيث لا يلزم ارتكابها التواجد في نفس المكان، كما يمكن ارتكابها في أكثر من دولة، وتختلف المواقيت الزمنية بين الدول، مما يُثير إشكاليات حول تحديد القوانين التي يجب تطبيقها على الجريمة الإلكترونية (ناصر, **2012**، ص**23**).

5. الخطورة الشديدة: تتميز الجريمة الإلكترونية بالخطورة الشديدة نظراً لأبعادها المتعددة والخسائر الضخمة التي تسببها. مقارنةً بالجريمة التقليدية، تستهدف الجريمة الإلكترونية المعنويات بدرجة أكبر من الماديات المحسوسة. كما تتميز بأنها تتضمن سلوكيات غير مألوفة وينفذها عدد من

الأفراد، مما يجعل تحديد المتسبب بها صعباً. بالإضافة إلى ذلك، ساعدت التكنولوجيا على تيسير ارتكاب الجرائم الأخرى، حيث تم ابتكار وسائل تجعل الكشف عن الجرائم التقليدية صعباً، خاصة إذا تم ارتكابها باستخدام أجهزة الكمبيوتر.

من خلال تحليل خصائص الجريمة الإلكترونية، يمكن فهم كيفية تميزها عن الجرائم التقليدية وتحدياتها الفريدة. تُظهر هذه الخصائص ضرورة تطوير استراتيجيات أمنية متقدمة وتعاون دولي فعال لمكافحة هذا النوع من الجرائم وحماية الأفراد والمؤسسات من تأثيراتها الضارة.

5.1أنواع الجريمة الإلكترونية

تعد الجريمة الإلكترونية من الظواهر الحديثة التي تطورت نتيجة للانتشار الواسع لشبكة الإنترنت والتقدم الكبير في مجال التكنولوجيا. هذه الجرائم تتميز بتنوعها وصعوبة اكتشافها، حيث تشمل العديد من الأنواع التي تستهدف الأشخاص، الأموال، والدولة ومؤسساتها. بناءً على العديد من الدراسات، يمكن تصنيف أنواع الجرائم الإلكترونية حسب الغرض منها على النحو التالي:

1. الجرائم التي تستهدف الأشخاص

يستهدف هذا النوع من الجرائم الضحايا بشكل مباشر، حيث يستخدم المجرم مختلف الأساليب لإلحاق الضرر بهم. تشمل هذه الجرائم:

أ. التهديد: يشكل التهديد جريمة بحد ذاته، حيث يُجبر الضحية على القيام بفعل أو الامتناع عنه مما يؤدي إلى ضرر على الضحية في ماله أو نفسه أو أفراد عائلته. يتم استخدام وسائل الاتصال مثل مواقع التواصل الاجتماعي (فيسبوك، إنستغرام، البريد الإلكتروني) لتنفيذ هذه الجرائم.

ب. انتحال الشخصية: أصبح الوصول إلى البيانات الشخصية للأفراد أسهل، وذلك من خلال محركات البحث والمواقع الإلكترونية. يمكن للمجرم استخدام هذه البيانات مثل الاسم الكامل، العنوان الشخصي، ورقم بطاقة الائتمان لانتحال شخصية الضحية وارتكاب الجرائم.

ت. السب والقذف: تنتشر هذه السلوكيات السيئة على مواقع التواصل الاجتماعي في التعليقات أو المنشورات بأشكال متنوعة (الصورة، الصوت، الكتابة)، مما يؤدي إلى ضرر معنوي ونفسي على الضحية نتيجة نشر معلومات مغلوطة عنها.

ث. المو اقع غير الأخلاقية: تهدف هذه المواقع إلى تفكيك النسيج الاجتماعي والقيم الأخلاقية من خلال تحريض على ممارسة الجنس للكبار والقصر، ونشر صور ومقاطع فيديو مخلة بالأدب.

2. الجر ائم التي تستهدف الأموال

تستهدف هذه الجرائم الأفراد والمؤسسات، خاصة مع التطور في التعاملات المالية عبر الإنترنت. تشمل هذه الجرائم:

أ. سرقة البنوك وحسابات الأفراد: تتم هذه السرقات من خلال اختلاس البيانات الخاصة بالضحية أو اختراق النظام المعلوماتي المالي للبنك، مما يسهل تحويل الأموال من حساب الضحية إلى حساب المجرم (سعدون وآخرون، **2011**، ص **4**).

ب. التجارات المحظورة: تتضمن التجارة المحظورة التي تمنعها القوانين الدولية، مثل تجارة المخدرات عبر الإنترنت أو التحريض على استخدامها أو صناعتها، بالإضافة إلى غسيل الأموال من خلال نقلها واستثمارها بطريقة تبدو قانونية.

3. الجر ائم التي تستهدف الدولة

تُوجه هذه الجرائم إلى الدولة ومؤسساتها مثل وزارة الدفاع الوطني ووزارة التعليم العالي والبحث العلمي. تشمل هذه الجرائم:

أ. الإرهاب السيبر اني: يستخدم الإرهابيون تقنية المعلومات لممارسة أنشطتهم الإجرامية من خلال وسائل الاتصال الحديثة، ونشر الأخبار المغلوطة لإثارة الفتنة وتحريك الرأي العام نحو الفوضى. يستهدفون الفئات الضعيفة مثل الأطفال والمراهقين الذين يكونون أول ضحايا السلطات القضائية بحكم مخالفة القوانين التشريعية للدولة (غريب، **2018**، ص **106**).

ب. التجسس: تعتمد الجماعات الإرهابية على جمع البيانات الخاصة بالمؤسسات الوطنية أو الدولية بطريقة غير قانونية، ومنحها للجهات المعادية للدولة. يتم ذلك من خلال الاطلاع على المعلومات الخاصة والمؤمنة في أجهزة المؤسسات ذات النشاط السياسي أو الاقتصادي أو العسكري والتي تعتبر معلوماتها من أسرار الدولة (محمد المايل ومحمد الشريجي، **2019**، ص **250**).

تعكس الأنواع المختلفة للجريمة الإلكترونية التعقيد والتطور الذي تشهده هذه الجرائم. من الضروري تطوير استراتيجيات أمنية فعالة وتعاون دولي لمكافحة هذه الظاهرة وحماية الأفراد والمؤسسات والدولة من تأثيراتها الضارة.

2تقنيات الجريمة الإلكتروني

1.2مفهوم تقنيات الاختراق الإلكتروني

يشير مفهوم التقنية إلى التطورات الحديثة الناتجة عن العولمة والتغيرات السريعة في المجتمع. هذه التقنيات مرتبطة بشكل كبير بالتكنولوجيا. ومع التطور الكبير الذي شهدته الجريمة بانتقالها من الواقع المادي إلى الواقع الافتراضي، ظهر العديد من التقنيات التي يعتمد عليها المجرم الإلكتروني في تنفيذ الهجمات الرقمية على البيئات الافتراضية وقواعد البيانات الخاصة بالجامعات والمستخدمين من الوسط الجامعي (نمديلي، **2017**، ص **5**).

ساهمت التكنولوجيا في تطوير تقنيات جديدة للاختراق الإلكتروني، مما يعزز قدرة المجرمين على تحقيق أهدافهم الإجرامية. يقصد بمفهوم تقنيات الاختراق الإلكتروني مختلف الطرق والمواد والبرامج والأجهزة الحديثة المستخدمة في العمليات الإجرامية التي تتم في الواقع الافتراضي، بهدف اختراق نظم المؤسسات الجامعية من خلال الاعتماد على الحاسوب والإنترنت. الهدف من هذه العمليات هو تخريب واختراق النظام المعلوماتي وإلحاق الضرر المادي والبشري بالمؤسسات التعليمية.

تتميز تقنيات الاختراق القائمة على الحاسوب بالعديد من المميزات التي تجعل من الصعب تتبعها والحد من خطورتها، نظرًا لسرعتها الفائقة ودقتها في إصابة الهدف. يعود ذلك إلى مستوى ذكاء المجرم وخبرته في مجال البرمجة والتعامل مع التقنية، إضافة إلى جودة الحاسوب وقوة معالجه. كما تلعب سرعة تدفق الإنترنت دورًا كبيرًا في عملية الاختراق، فكلما كانت سرعة التدفق أكبر كانت عملية الاختراق أسرع وأكثر خطورة على المؤسسات التعليمية (بن جدو، **2022**، ص **304**).

إضافة إلى ذلك، تتميز تقنيات الاختراق بالدقة والمرونة وعدم الخطأ، وذلك يعود لتصميمها الفريد وعملها الآلي الذي يتم ضبطه عبر الحاسوب. ومن مميزاتها عدم التعرض للملل أو الإرهاق كما يحدث مع الإنسان، ولكن قد تخرج عن الخدمة في حالة حدوث خلل تقني في البرنامج أو الحاسوب، أو في البرمجة أو نظام التشغيل أو المعلومات المدخلة.

بناءً على ما سبق، يمكننا تعريف تقنيات الاختراق الإلكتروني كنموذج جديد في الجريمة نتيجة للتطور التكنولوجي. تعتمد هذه التقنيات على البرامج والتطبيقات والبرمجة الحديثة لاختراق الأنظمة المعلوماتية. ولنجاح عملية الاختراق، يتطلب توفر المجرم كقائد للعملية، بالإضافة إلى الحاسوب والإنترنت. يتم الاختراق من خلال برمجة تطبيقات توجه فيروسات وتبحث عن الثغرات والشفرات التي تسمح لها بالتسلل إلى النظام المعلوماتي الخاص بالجامعة أو الحسابات الشخصية لأفراد الوسط الجامعي.

في الختام، تعتبر تقنيات الاختراق الإلكتروني جزءًا لا يتجزأ من التطور التكنولوجي الحديث، مما يستدعي تعزيز الإجراءات الأمنية لحماية المعلومات والبيانات في المؤسسات التعليمية. يتطلب ذلك تعاونًا دوليًا وتطوير قوانين وتشريعات تواكب هذا النوع الجديد من الجريمة، بهدف التصدي بفعالية لتحديات العصر الرقمي.

2.2. أنواع تقنيات الاختراق الإلكتروني

تشكل تقنيات الاختراق الإلكتروني تهديد على أمن المعلوماتي للمؤسسة الجامعية وأفرادها حيث تتعدد نماذجها وأشكالها المهددة، التي تشكل خطر على الأمن المعلوماتي وقواعد البيانات الخاص بالمؤسسة التعلمية، فيما يتعلق بمحتوي الشبكة العالمية والحاسب الآلي ونظام البيانات ومن بين التقنيات الأكثر استعمالا من طرف مجرمي الأنترانت نجد:

1.2.2. تقنية Denial Of Services (DOS)

يتم تنفيذ هجوم انقطاع الخدمة عن طريق إغراق الجهاز الضحية بطلبات الاتصال أو أوامر بروتوكول الشبكة للإغراق بمعالجة هذه الطلبات، مما يتسبب في تجاوز الكمبيوتر لقدراته حتى يتوقف عن الاستجابة، وبالتالي لا يمكنه أداء مهامه مدى إغراق Hooding هو تعطيل الهدف بشكل دائم وإخراجه من الخدمة، تستهدف هجمات رفض الخدمة ثلاثة أنواع مختلفة منها المستخدم والكمبيوتر المضيف والشبكة، بدأت هجمات رفض الخدمة باستخدام الأدوات المنقولة عبر الإنترنت، مثل Tribe Flood Network وStacheldraht، وهي أداة تصدر أوامر لأجهزة الكمبيوتر، التتابع حتى يتوقف عن الاستجابة ، ثم يمكن استغلال ثغرة أمنية للحصول على وصول غير مصرح به إلى البيانات أثناء توقف الكمبيوتر، وبعض الطرق لإفساد البيانات وتعطيل الخدمة ومنع المستخدمين الشرعيين من الوصول إليها .(**Goutam, 2015, p. 15**)

2.2.2. تقنية Social Engineering

الهندسة الاجتماعية هي فن مخادع للتواصل مع الأشخاص للحصول على معلومات مهمة، في شكل سرية، معظم الناس لا يعرفون قيمة المعلومات التي لديهم، لذلك وجدنا أن المهاجمين يستخدمون العديد من الأساليب المختلفة، للإقناع الضحايا بتمرير المطالبات أنه مسؤول معترف به لتقديم هذه المعلومات، كما في حالة سرقة أرقام بطاقات الائتمان، يتظاهر المهاجم بأنه موظف مصرفي في بنك معروف ثم يسأل الضحية، عن رقم بطاقته الائتمانية أو رقم هويته الشخصية. (Salahdine & Kaabouch, 2019, p. 2)

3.2.2. تقنية Phishing

تتمثل الطريقة النموذجية للجمع بين عمليات الاحتيال في الهندسة الاجتماعية وتكنولوجيا الويب من خلال إنشاء موقع ويب مزيف لموقع ويب موجود بغرض خداع المستخدمين، عادةً من خلال رسائل البريد الإلكتروني العشوائية، ورسائل الهاتف المحمول والإعلانات الكاذبة التي تظهر أثناء تصفح موقع الويب، محتوى الموقع واستخدامها لسرقة حسابات البريد الإلكتروني، أو أرقام الحسابات المصرفية وغيرها من المعلومات الهامة، ينخدع المستخدم بالمعلومات الخاطئة أعلاه ،والتي تحتوي على روابط لمواقع مزيفة تشبه الموقع الأصلي فينتقل المستخدم إلى هذه المواقع ويملأ البيانات، التي كتبها أثناء تصفحه للموقع الأصلي مثل حسابه البنكي معلومات أو معلومات أخرى مهمة عن موقع الويب، لذا فإن المستخدمين الساقطين هم ضحايا جرائم التصيد، لأن موقع الويب المزيف هو نفسه في الواجهة الرئيسية للموقع الأصلي ، مثل التصميم واللون والشكل، وما إلى ذلك يمكن أن يكون موقع الويب المزيف مختلفًا عن الأصلي مع تمييز بسيط كحرف علامة زائد أو ناقص(Alkhalil et al., 2021, p. 2)

4.2.2. تقنية Malware

تعد من البرمجيات الخبيثة من أكبر الهجمات على أنظمة المعلومات التي تصيب أجهزة الكمبيوتر والهواتف المحمولة المتصلة بالإنترنت، ترخيص بغرض إحداث ضرر أو تعطيل أو اتخاذ أي إجراء غير قانوني ضد المعلومات الواردة في جهاز الضحية. (Ucci et al., 2019, p. 6)

5.2.2. تقنية Spyware

برامج التجسس هي نوع آخر من البرامج الضارة لأغراض غير قانونية، يراقب كل شيء يكتبه الضحية لتسجيل ضغطات المفاتيح، وإرسالها إلى المتسلل كما يقوم بتنفيذ إجراءات ضارة أخرى، وهو

يؤدي المهام بشكل مستقل عن طريق الاتصال بالشبكات الاجتماعية أو مواقع الويب وتقوم هذه البرامج بجمع معلومات، حول نشاط المستخدم على جهاز الضحية، سواء عبر الإنترنت أو دون اتصال بالإنترنت، وعندما يكون الكمبيوتر متصلاً بإرسال هذه المعلومات إلى المخترق مباشرة بعد الإنترنت (**Egele et al., 2007, p. 234**)

6.2.2. تقنية Spamming

البريد العشوائي في هذا النوع من الهجوم، يتم استخدام البريد الإلكتروني كوسيلة لإغراقه بالرسائل الإعلانية لمنتجات معينة، وهذا يستهلك موارد الكمبيوتر ويتطلب الكثير من الوقت والمال، مما قد يؤدي إلى تعطيل الشبكة وإبطاء سرعات نقل البيانات إلى الإنترنت بسرعة الإرسال والاستجابة للخدمة نفسها، تم اختيار البريد الإلكتروني كبيئة لشن هذا النوع من الهجوم لأن العلاقات الاجتماعية الموجودة بين المستخدمين، وخاصة في مواقع التواصل الاجتماعي تقوم على الثقة الزائفة، مما يعني أنه من السهل إقناع المستخدمين المستهدفين بقراءة محتوى البيانات غير المرغوب فيه، مثل هذا يخلق الوهم بأنها رسائل أمنية لذلك يمكن أن تتطور هذه الهجمات إلى جرائم تصيد احتيالي.(**Hayati et al., 2010, p. 581**)

3.2. المشكلات الناتجة عن تقنيات الاختراق الإلكترونية

بالرغم من الإيجابيات الهائلة لشبكة الإنترنت وتقنياتها، التي سهّلت الحياة المادية للفرد من حيث التواصل والعمل، فإن الواقع الافتراضي يمثل مزيجًا بين الأفراد الذين يستخدمون الإنترنت بشكل قانوني، وفئة أخرى تعتمد عليها لتحقيق أهدافهم بطرق غير مشروعة. وهكذا هو الإنترنت؛ على الرغم من مزاياه العديدة، إلا أنه له جانبه المظلم.

تزداد جرائم الإنترنت يومًا بعد يوم، وتظهر بأشكال مختلفة ومتنوعة، حيث يعتمد المجرمون على العديد من التقنيات لإنجاز مهامهم غير القانونية، مما يؤدي إلى فقدان الحياة، والكرامة، والوظيفة. لا يقتصر تأثير جرائم الإنترنت على الضحية فقط، بل يمتد تأثيرها إلى المجتمع ككل. تشمل عواقب جرائم الإنترنت على الاقتصاد فقدان الإيرادات، وضياع الوقت، وتلف السمعة، وانخفاض الإنتاجية، وغير ذلك (**Igba et al., 2018, p. 1146**).

ومن المشاكل الناتجة عن التقنيات هو الاختراق الإلكتروني. حسب دراسة دانيال إيجا وآخرين (2018) للمؤسسات الدولية وأفرادها، تتجلى تأثيرات هذه الجرائم على النحو التالي:

1.3.2. فقدان الإيرادات

أحد التأثيرات الرئيسية لجرائم الإنترنت وتقنياتها على الاقتصاد الوطني والدولي هو فقدان الإيرادات. على سبيل المثال، في المؤسسات المالية الوطنية أو الشركات العالمية، يمكن أن يتسبب تسريب معلومات مالية حساسة من قبل طرف خارجي في سحب الأموال من حساب هذه المؤسسة. كما يمكن أن تحدث جرائم الإنترنت عند اختراق موقع تجارة إلكترونية خاص بشركة، وعندما يصبح غير قابل للتشغيل، فإن الدخل القيم يضيع عندما يتعذر على المستهلكين استخدام الموقع، مما يؤدي إلى خسائر مالية كبيرة للشركة

2.3.2. تضرر السمعة

في الحالات التي يتم فيها اختراق مؤسسات مثل البنوك، مما يعرض سجلات العملاء للاختراق الأمني، يمكن أن يؤثر هذا النوع من الجرائم على سمعة الشركة. فعندما يكون نظامها وبنيتها المعلوماتية غير آمنة، تتعرض بطاقات الائتمان أو البيانات المالية للعملاء للاختراق من قبل المتسللين أو القراصنة الإلكترونيين. يؤدي ذلك إلى فقدان الثقة في المؤسسة، مما يدفع العملاء إلى الانتقال إلى مؤسسات أخرى توفر لهم حماية أفضل للممتلكات المالية، مما يسبب خسارة مادية وتشويهًا لسمعة الشركة.

3.3.2. انخفاض الإنتاجية

تستوجب على الشركات والمؤسسات ذات النشاط الاقتصادي والمالي اتخاذ جملة من الإجراءات لمكافحة جرائم الإنترنت. غالبًا ما يكون لهذه الجرائم تأثير سلبي على إنتاجية وعمل الموظفين من ناحية الأداء والنفسية. فكلما كان المحيط الافتراضي المهني للعامل آمنًا، زادت راحته وحقق له الرضا الوظيفي، مما يجعله أكثر إنتاجية ويعود بالنفع على المؤسسة.

4.2. أسباب الوقع ضحية للجريمة الإلكترونية

الجريمة الإلكترونية هي من الأفعال الغير المشروعة، التي تعاقب عليها القوانين التشريعية في الجزائر، فلا يوجد تميز بين الجريمة الإلكترونية والجريمة التقليدية، فأبرز اختلاف هو مسرح الجريمة الذي يعتبر الوسط الافتراضي، فمن أسباب ظهورها هو التحول الرقمي والعولمة، أما من أسباب انتشار الجريمة فيه هو تطور تقنياته وانتقال السلوك من الواقع المادي الى الافتراضي، ويمكن لنا تصنيف عديد من الأسباب التي تجعل من مستخدمي الأنترانت ضحيا للأنواع من الجريمة الإلكترونية:

1.4.2. الخبرة التقنية للمجرم

يستعمل كل من المجرم والضحية الكمبيوتر، كوسيلة للاتصالي بالواقع الافتراضي أما الفروق التي بينهم في مدي تمكنهم في استخدام، الحاسوب كأداة فالمجرم يستغل الضعف للفرد الذي يستهدفه، ويكون الضرر الذي يلحق كبيرًا نسبيًا وغير ملموس للأنه في الواقع الافتراضي مما يجعل من الصعب اتخاذ إجراء قانوني ضد هذه الجرائم، فكلما كان مستوي المعرفية التقنية عالي بنسبة للمجرم ادي هذا الى زيادة من مجموعة الضحايا المحتملين، وتجعل من الصعب تعقبه وإلقاء القبض عليه إضافة الى حداثة هذا نوع من الجرائم، أدي الى عدم جاهزية المجتمع بشكل عام الى عدم قدرة على مكافحتها بنفس القدرة.(خليلي, **2018ص406**)

2.4.2. ضعف الحاسوب

باعتبار الحاسوب معرض للضعف هنالك العديد، من الأسباب الرئيسية التي لتجعله عرضة لتقنيات الاختراق المستعملة من طرف المجرم، هي القدرة على تخزين البيانات في مساحة صغيرة نسبيًا حيث تتمتع الحواسيب بخاصية فريدة من نوعها، لتخزين البيانات في مساحة صغيرة جدًا، وهذا يتيح إزالة أو استخلاص المعلومات، إما عن طريق الوسائط المادية أو الافتراضية مما يجعل الأمر أسهل بكثير(**Dashora, 2011, p. 242**).

فالوصول السهل حيث تكمن المشكلة التي تواجه حماية نظام الكمبيوتر، من الوصول الغير المصرح به مما يأدي به إمكانية للخرق من طرف المجرمين الإلكترونيين، يكون اما بسبب بشري ولكن بدرجة الأولى، يكون بسبب التكنولوجيا المعقدة، من خلال استخدام قنابل البريد الإلكترونية، أو برامج الخبيثة التي يمكنها سرقة رموز الوصول لنظام التشغيل خاص بالجهاز وجعل فيه ثغرات تسهل عملية التسلل الإلكترونية، ومحاكات الصوت المتقدمة، والماسحات الشبكية، وما إلى ذلك التي يمكنها اختراق أنظمة أمان كثيرة.

3.4.2. خاصية التعقيد بنسبة للأنظمة التشغيل الخاص بالحاسوب

حيث يعمل الكمبيوتر على أنظمة تشغيل، وتتألف هذه الأنظمة من ملايين الأكواد العقل البشري قابل للخطأ، ومن غير الممكن عدم حدوث خطأ في أي مرحلة، يستغل المجرمون الإلكترونيون هذه الثغرات ويخترقون النظام الكمبيوتر، كما يلعب الأهمال بنسبة للمستخدم كونه مرتبط جدًا بالسلوك البشري، لذلك فمن المحتمل جدًا أن يحدث أي إهمال أثناء حماية نظام الكمبيوتر، ويمكن أن يمنح المجرم الإلكتروني الوصول والتحكم في نظام الكمبيوتر(رابحي **2018**،ص**112**).

وفي الأخير يمكن اعتبار غياب الأدلة من المشاكل، التي تصعب منها في كشف عن المجرم حيث يتعمد المجرمون الإلكترونيين تدمير جميع البيانات بشكل روتيني، وتعطيل جميع البيانات خارج النطاق الإقليمي هذا النظام للتحقيق في الجرائم.

5.2. إستراتيجيات الوقاية من جرائم الإنترنت

أصبحت الوقاية من الجريمة والتهديدات السيبرانية بنسبة للمستخدمين الأنترانت نتيجة الانتشار الواسع لها في الواقع افتراضي، وأصبح الوضع الراهن يفرض اتخاذ الاحتياطات المناسبة لكل نوع من الهجمات السيبرانية، التي تهدد حواسيبهم وهواتفهم وكل بياناتهم الرقمية ومن الضروري رفع الوعي بجرائم الإنترنت، وتقليل آثارها من خلال ضمان حصول جميع طلاب الحوسبة على معرفة واسعة وحديثة.

حيث يعرف أبو ساق (2013) الوقاية "بمجل التدابير النظامية التي غايتها التخلص من أسباب الجريمة الإلكترونية" (أبو ساق **2013**، ص**125**) ومنه فاستراتيجيات الوقاية من جرائم الأنترانت ترتكز على العناصر الأساسية التالية:

1.5.2. مستوى الثقافة الرقمية

ترتبط كل من الوقاية والامن الرقمي، بمستوى الثقافة التقنية للمستخدم على الإنترنت في استخدام الحاسوب حيث عرفها محمد النجار (2013)' بأنها مجموعة من القيم والمعارف والمهارات الرقمية التي يجب على الفرد اللمام بها في ظل تطور التكنلوجي" (النجار**2013**،ص **16**)

وبهذا فالأنترانت تعتمد على تقنية الحاسوب، وهي تتأثر بمستوي مهارات المستخدم وثقافته التقنية من خلال اختياره للمواقع الأمنة، عند التصفح ومدي إمكانيته في كشف ان كان موقع مزيف او مفترسة خاصة عند التسوق الإلكتروني، حيث تكون معاملات مالية وتفر على مستخدم استعمال بيانات رقمية للهويته ولبطاقة الائتمان.

2.5.2. استخدام برامج الأمن

استخدام الأنترانت يفرض على مستخدم توفير محيط أمن عند التفاعل الافتراضي، من خلال استخدام مجموعة متنوعة من التطبيقات، عند الاتصال بالأنترانت من أجل للترفيه والتسلية والاتصال أو لمهام العمل، لتجنب اختراق البيانات و الخصوصيات في حالة تعامل خاطئ مع المحتوى الغير لائق

الذي يتم استرداده عن طريق الخطأ، من خلال رسائل البريد العشوائي، او من تطبيقات التجسس او عند ضبط خيارات الخصوصية والأمان للمتصفح وغيرها ، مثل البنية التحتية للمفاتيح العامة، وكاشفات الاختراق، والوقاية من خلال جدران الحماية، ومكافحة الفيروسات، ومكافحة البريد المزعج وبرامج التجسس.

3.5.2. الدور التكاملي للتحقيق الأمن الافتراضي

يمكن للدور التكاملي بين الأجهزة الأمنية ومستخدمي الأنترانت، من المواطنين تحقيق شعور بالأمن ويمكن تجسيد هذا من خلال الحد من جرائم الإنترنت، عن طريق الإبلاغ عن أي شخص يتورط في جرائم الإنترنت للجهات الأمنية مما يسهل للجهات الأمنية من تولى الفعل الممارس من خلال الردع القانون والسيطرة على الجاني، إضافة الى هذا، يستوجب على السلطات الأمنية أبرام العديد من الندوات والملتقيات لعلمية والتوعوية حول ظاهرة الجريمة الإلكترونية حيث يساهم من تنمية وعي المواطن بمخاطرها.

3.ماهية الوسط الجامعي

1.3. مفهوم الوسط الجامعي

الجامعة هي مؤسسة تعمل على تنمية وتنشئة أفراد المجتمع في أعلى مستوياته. فهي تعد من أهم المؤسسات الاجتماعية التي تؤثر وتتأثر بالبيئة الاجتماعية المحيطة بها، إذ إنها من صنع المجتمع وأداته في صنع قيادته الفنية، والمهنية، والسياسية، والفكرية. لكل جامعة رسالتها الخاصة التي تسعى لتحقيقها، ولكل نوع من المجتمعات جامعته التي تناسبه من حيث اتصال الجامعات بمجتمعاتها وتقديم مجموعة من الأدوار، والأنشطة، والخدمات لهذا المجتمع. أصبح هذا الأمر ضرورة تفرضها المتغيرات المعاصرة، فالجامعة هي معقل الفكر الإنساني في أرفع مستوياته، ومصدر لاستثمار وتنمية أهم ثروات المجتمع وأغلاها وهي الثروة البشرية (راشد، **2008**، ص. **12**).

مع تطور التكنولوجيا واستخدام الإنترنت، تأثرت الجامعات بشكل كبير، مما أدى إلى تغيير نمط التعليم التقليدي. هذا التحول من التعليم التقليدي الذي يعتمد على المحاضرات التفاعلية بين الأستاذ والطالب في قاعات الدرس التقليدية إلى التعليم الإلكتروني أصبح ضرورة ملحة. التعليم الإلكتروني يقوم أساسًا على استخدام الحاسوب والإنترنت، حيث يتم التفاعل بين الطالب والبرنامج التعليمي، وأحيانًا بين

الطالب وعضو هيئة التدريس. تطورت أدوات التعلم الإلكتروني لتشمل النص، والصورة، والفيديو، والصوت، والألعاب، مما يثري تجربة التعلم الإلكتروني ويجعلها أكثر تفاعلية وشمولية (شمام، 2022، ص. 15).

إن ربط الوسط الجامعي بالإنترنت لم يؤثر فقط على نمط التعليم، بل غير أيضًا طبيعة التفاعل بين الفاعلين الأساسيين في الجامعة: الطلبة، والهيئة التدريسية، والإدارية. الاعتماد على الوسائط الإلكترونية أصبح أمرًا لا مفر منه، حيث تتضمن هذه الوسائط مجموعة من التطبيقات العملية التي تقوم على أسس التكنولوجيا الرقمية وتعتمد على الشبكة العنكبوتية. هذه الوسائط تسمح بإنتاج المحتوى وتعديله، كما تتيح للأفراد والمجموعات نشر المواضيع، ومناقشتها، ومشاركة الآراء بشكل مباشر، مما يعزز التواصل الفعال بين مكونات المجتمع الجامعي.

علاوة على ذلك، تساهم الجامعة في تطوير البنية التحتية للمجتمع المحلي، وهو أمر ضروري لتعزيز التعليم الجامعي والبحث العلمي. الجامعة تسعى دائمًا لخدمة المجتمع والارتقاء به حضاريًا من خلال تزويده بالمختصين والفنيين والخبراء في مختلف المجالات. تقوم بإعداد موارد بشرية مزودة بأصول المعرفة، وطرائق البحث المتقدمة، والقيم الرفيعة، مما يساهم في بناء وتدعيم المجتمع وصنع مستقبل الوطن وخدمة الإنسانية. للجامعة ثلاث وظائف أساسية تسعى لتحقيقها: التعليم، والتدريس، وخدمة المجتمع (الزكي، **2007**، ص. **160**).

نظرًا للدور الحيوي الذي تلعبه الجامعات في تطور المجتمع، فإنها تبقى تحت تهديد الهجمات الإلكترونية. الربط بالإنترنت وتحول البنية المادية للجامعات إلى بنية افتراضية يزيد من التفاعل بين الفاعلين في الوسط الجامعي ويتيح نوعين من التفاعل: الواقعي، والتفاعل عبر الوسائط الإلكترونية. مع تطور الجريمة الإلكترونية، أصبح كل تحدٍ يواجهه الأفراد في الواقع متمثلًا أيضًا في الفضاء الإلكتروني، مما يفرض على الجامعات اتخاذ تدابير وقائية لتعزيز أمنها السيبراني وضمان استمرارية دورها التعليمي والتنموي في المجتمع.

2.3. وظائف الوسط الجامعي.

الجامعة من المؤسسات العليا في أي دولة، وهي أساس بناء الوعي بكل أنواعه بنسبة للمجتمع وكشف الحقيقة له من خلال النشر العلمي، وتكوين جيل قادر وكفء في قيادة الوطن نحو التقدم من خلال توسع نطاق المعرفة الإنسانية، للخروج من التخلف والتبعية الفكرية والاستلاب الثقافي، والعاملة

على إثبات الهوية الوطنية وتحقيق التطور في جميع المجالات حيث تعمل الجامعة الجزائرية، وكل أفراد الوسط الجامعي على تحقيق وظائفها الأساسية على أرض الواقع وهي على النحو التالي:

1.2.3. الوظيفة التدريسية

وهي من الوظائف البيداغوجية الخاصة بالمؤسسة الجامعية ككيان قائم بذاته ويتم تجسيد هذه الوظيفة من خلال عملية الاتصالية بين الطالب والأستاذ، أضافة الى البرنامج التعليمي المعتمد في التأطير، من طرف وزارة التعليم العالي والبحث العلمي وبهذا فهي شبكة من العلاقات الاجتماعية والثقافية والفكرية، بين الأستاذ والطالب مهمتها تكوين عادات واتجاهات وممارسات تعكس حقيقة المجتمع الجامعي ومواصفات الحياة الجامعية.

فالعملية التدريسية تركز على تكوين الطالب بالمعرفة، في جميع العلوم بجانبيها النظري والتطبيقي وتهيئة الظروف الداخلية والخارجية، له للأكسابه الخبرة اللزمة تسمح له الاندماج في الحياة العملية. **(بولشفار 2018، ص 345)**

2.2.3. الوظيفة العلمية

تجمع الوظيفة العلمية بين كل من البحث العلمي، والعملية التعليمة فكل منهما يحقق للجامعة أهدافها المواجهة للبناء البنية البشرية، في جميع العلوم وتجاهل أحد هذين العنصرين يخرج الجامعة عن رسالتها الأساسية وكيانها العلمي، فمن خلال البحث العلمي يمكن للدولة أن تتطور في كل من الجانب الاقتصادي، والتكنولوجي والصحي، ويحقق لها الاستقرار السياسي وتحقق بذلك أمنها الداخلي والخارجي. **(غربي, 2014, ص 15)**

3.2.3. الوظيفة الاقتصادية

يعتبر مشروع الاقتصاد المعرفة من المشاريع الواعدة، التي تعمل عليه السلطات العليا في الدولة الجزائرية من خلال توفير تكوين جامعي على مستوي عالي، و دعم مادي يسمح للطالب من خلال التكوين الجامعي، في طورين لسانس و ماستر أن يأسس مؤسسة ناشئة خاصة به، تأهلهم لقيادة الاقتصاد الوطني من خلال تحقيق الاكتفاء الذاتي ومساهمة في فتح مناصب شغل، وعليه يمكن القول أن الوظيفة الاقتصادية للجامعة أساسية في إعداد إطارات التي يحتاجها سوق العمل، للخروج من استيراد الخبرة الأجنبية كما تستورد الأجهزة الصناعية والتكنولوجية. (اسماء و شابونية **2019**،ص **170**)

4.2.3. الوظيفة السياسية

تدخل الوظيفة السياسية للجامعة في مهام بناء الفكر، وتكوينه بنسبة للمجتمع نتيجة الصراعات الأيديلوجية التي تشهدها المجتمعات، في جميع أنحاء العالم حيث يعتبر عنصر أساسي للتحقيق الأمن الوطني القوي، وتطور الدولة حيث أن الصراع الأيديولوجي ادي بالعديد من الدول الى حروب أهلية، ودور الجامعة يبرز في ترسيخ سياسة تتماشي مع أساس الدولة ودينها الإسلامي ومبادئ التي عمل جبهة التحرير الوطني، وشهداء الوطني على تحقيقها والحفاظ عليها.

3.3. مكونات الوسط الجامعي

تعتبر المؤسسة الجامعية مؤسسة متكاملة، تجمع بين ثلاث بنيات أساسية وهي البنية البشرية والمادية والمعنوية، التي تضمن لها كيانها واستمرارها لتحقيق أهداف الرئيسية، ومن مكونات الوسط الجامعي هي كمايلي:

1.3.3. البنية البشرية للوسط الجامعي

البنية البشرية هي جزء أساسي من عناصر الإنتاج العلمي والتكوين والتنظيم في مؤسسة الجامعية وهو يشير إلى جميع العاملين، في المؤسسة بما في ذلك الإدارة والموظفين والطلبة والعاملين على العقود والمتعاقدين من الأساتذة، والذين يساهمون جميعًا في تحقيق أهداف المؤسسة الجامعية ومن مكوناتها هي:

أ-الاداريون: تحتاج كل مؤسسة جامعية إلى تنظيم إداري يرتكز على الخبرات السابقة ويضمن نجاحها على المدى الطويل، يقوم العمل الإداريون حسب الكليات والأقسام بمراقبة تحقيق أهداف المؤسسة داخل إطار التنظيم، ويتعين عليهم التكيف مع المتغيرات التي تحدث في المؤسسة من خلال التسيير المالي والإداري داخل الوسط الجامعي، وتوكل لهم المهام البيداغوجية وتختلف من عامل الى أخر حسب تصنيفهم داخل تنظيم الجامعة. (سعودي **2010**،ص **39**)

ب-الأساتذة: وهم الحلقة الأساسية في العملية التكوين العالي، حيث ينقسم الى ثلاثة أقسام (أستاذ مساعد، أستاذ محاضر، وأستاذ تعليم عالي) ويتم ترقيتهم حسب الخبرة العلمية والإنتاج العلمي، حيث توكل لهم مهمة التكوين والتدريس الطالب من خلال المحاضرات، وحصص الموجهة والأشراف على أطروحات تخرجهم في مرحلة لسانس وماستر، ودكتوراه إضافة الى النشاطات العلمية مثل الملتقيات الوطنية والدولية. (صالح والعجيلي **2013**،ص **91**)

ت-الطالب: يعتبر الطالب الحلقة الأساسية، في هيكل التنظيمي للمؤسسة الجامعية حيث يتم التفاعل بين كل من الوظائف البيداغوجية والتعلمية لكل من الأدريون والأساتذة، من أجل تكوينه وتوفير له محيط تعليمي من أجل اكسابه كل المهارات المتعلقة بالحث العلمي، والعملي بشقيها النظري والتطبيقي ليكون فرد قادر على الاندماج في الحياة العملية بعد التخرج من الجامعة. (نجار **2003**، ص **964**)

2.3.3. البنية المادية للوسط الجامعي

تتمثل البنية المادية في بنية الجامعة، ومختلف الهياكل المادية التي يحتويها هذا البناء من قاعات التدريس، ونوادي والتنظيمات الطلبية وإدارة بأقسامها وكلياتها وملاعب ومكتبة بالإضافة إلى الوسائل التعليمية، والبيداغوجية التي تعتمدها الجامعة في تأدية مهامها.

3.3.3. مكون المعنوي للوسط الجامعي

ينظم الطرف المعنوي كل من المناهج والمقررات، و البرامج التعلمية موجهة لكل الفاعلين في الجامعة إضافة الى مجموعة من المعاير والقوانين والقيم التي يستوجب منهم احترامها والسير عليها لضبط سلوكهم وتنظيم، مهامهم في الجامعة بسبة لكل فرد حسب منصبه و مكانته داخل الهيكل تنظيمي. (بوفلجة **2006**، ص **77**)

4.3. أهداف الوسط الجامعي

انا من متطلبات التطور الورقي في الجانب التكنولوجي والاقتصادي، يستوجب أتباع المعاير العالمية لسير في ركب دول المتقدمة، ولن يكون هذا الى من خلال الجامعة باعتبارها المؤسسة الأولى، في دولة مكونة للأطارتها البشرية ونخبتها حيث تخضع الأهداف المرسومة في الجامعات إلى الطبيعة السياسية والاجتماعية، لكل المجتمع وواقعه ومشكلاته وهذا التفاوت طبيعي وينتج عن اختلاف الفلسفات، التي تقوم عليها مثل هذه المؤسسات الجامعية واختلاف المواقف وأهداف النظام الحاكم التي يتخذوها مسيري الدولة.

ومن العناصر الأساسية للأهداف الجامعة التي تعمل على تحقيقها هي:

1.4.3. التنمية البشرية

نعني بها الاستثمار في البناء الاجتماعي، من خلال التعليم والتكوين من تحسين مستواه الفكري والعلمي للتحقيق الإنتاج والتطور وراقي، هذا مجموعة من الأسس التي يستوجب السير عليها على مدي

طويل حتي يتحقق شرط المداومة في تطور من خلال تحسين المناهج الدراسية و جودتها لضمان الاستقرار وتثقيف للمورد البشري و حمايته، فكريا وصحيا و تحقيق أمنه في كل جوانب الحياة، عن طريق الأبحاث التي تنجزها الجامعة حيث يتم تبسيط معارفها بالمستوى الذي يسمح بتوصلها، وتبليغها إلى العامة من الناس وهذا بدوره يساهم في توثيق الصلة بين الجامعة، والواقع الإنساني والمادي للمجتمع. (شبل ونجيب **2006**، ص **36**)

2.4.3. التطور التكنولوجي

ان التطور التكنلوجي في الوقت الراهن، أصبح هو حلق الصراع للدول في جانب سباق الفكرة واكتساب المادة للتصبح المتحكمة والمسيطرة وبسط قوتها من خلال الابتكار في العلم والتقنية وتنويع الأدوات، والطرق للإنتاج معرفة جديد لخدمة البشرية، وتسهيل حياته من خلال:

أ-العمل على تفعيل العلاقة بين العلم والبحث العلمي في الحياة الاجتماعية

ب-تنمية القدرات الطالب من خلال إعطاء فرص الإبداع والابتكار مثل مشروع اقتصاد المعرفة التي أقرته الحكومة والرئيس الجمهورية الجزائرية.

ت-تعميم التكنولوجية في حياة المواطن وخاصة بنسبة للمنصات الرقمية التي أصبحت تنشئها الدولة الجزائرية لدمج التكنولوجيا في حياة اليومية.

ث-العمل على تحديد الأهداف التكنولوجية (التطبيق والتطور، المحاكاة) والابتكار من خلال تشجيع على البحث العلمي والنشر العلمي ودعم المشاريع العلمية.

3.4.3. التنمية الاقتصادية

التنمية الاقتصادية للدولة تستوجب الجمع بين العلم والمورد البشري، ليسهل عملية مواكبة التكنولوجية الحديثة وهي من مهاهم الجامعة، عن طريق استنباط أساليب إنتاجية جديدة لإنماء المهارات و الطاقات البشرية إضافة إلى زيادة المداخلات المالية في المجتمع، و من ثم فإن التنمية الاقتصادية تنطوي على تغيرات اقتصادية، و اجتماعية و هيكلية و تنظيمية حيث كذلك تشمل تحسين كل من مهارة وكفاءة و قدرة العامل على الحصول على الدخل و تنظيم الإنتاج بطريقة أفضل ، و تطوير وسائل النقل و المواصلات، و تقدم المؤسسات المالية، إضافة إلى زيادة معدل التحضر و تحسين مستوى

الصحة والتعليم التعليم العالي الجامعي يعتبر نوع من أنواع الاستثمار، و الذي اهتم به رجال الاقتصاد في التنمية الاقتصادية. (العلمي وروابحي **2017**،ص **213**)

5.3.تدابير الحماية الوسط الجامعي من الجريمة الإلكترونية

يبقي الوسط الجامعي دائما تحت تهديد عديد من الهجمات الإلكترونية التي تشكل خطر على مكوناته المادية والبشرية وأضرار على تجهيزاته، من حواسيب وشبكة العنكبوتية ونظامه المعلوماتي ولهذا يستوجب على القائمين على المؤسسة الجامعية أخذ الحيطة، من خلال انتهاج التدبير اللزمة التي يمكن من خلالها مواجهة تقنيات الاختراق، التي يعتمد عليها مجرمي الأنترانت (ذياب،**2014**، ص**14**) وهذا من خلال التنظيم للوسط الجامعي، وحماية الخصوصيات والتوفير الحماية وهي على النحو التالي:

1.5.3.تنظيم الوسط الجامعي

تنظيم الوسط الجامعي يعتبر من وظائف الأدراة الجامعية بحكم لكل مؤسسة هيكل تنظيم مختلف عن الأخرى نتيجة للوظائف المقدمة، او للمجال الذي تتخصص فيه اما باعتبار الجامعة من المؤسسات المعتمدة، في مجال التعليم والتكوين العالي فتنظيمها وتفاعلها يشمل جميع المجالات، للأن موكل اليها تكوين وتأهيل الكفاءة في مستوي عالي لهذا يتوجب عليها ربط علاقة على مستويين الداخلي، وخارجي للتحقيق الجودة والتطور للكن في اطارة ما يوجهها من مخاطر الكترونية تفرض عليها تنظيم محكم للأنشطة الإدارية، وهذا لسيطرة على نظام المعلومات للجامعة وقواعدها البيانية من التحكم ببرامجها الخاصة، والأشراف والمتابعة على أنشطة المؤسسة في شقيها الداخلي والخارجي والرقابة، من خلال انتهاج مجموعة من التعليمات والارشادات، التي تكون في اطار الحماية المعلوماتية من مخاطر الإلكترونية وهذا لضبط السلوك بنسبة للعاملين والطلبة داخل الوسط الجامعي، وزيادة وعيهم تجاها تدابير الحماية والموجهة بنسبة لتقنية الجريمة الإلكترونية (جبرا، **2015** ص**122**).

2.5.3. حماية الخصوصيات

تدخل في أطار حماية الموظفين والعاملين ومنتمين ومسجلين، في النظام المعلوماتي للجامعة وبما نسميه حماية البيانات والمعلومات الشخصية للأفراد، بحكم هم الحلقة الأساسية للوسط الجامعي وهم عرضة لتهديدات الإلكترونية، كما يمكن أن يكون سبب فيها نتيجة لخطاء الاستخدام لوسائط الإلكترونية المتصلة بنظام المعلوماتي، لهذا فحماية خصوصياتهم من طرف الجامعة تكون من خلال الاعتماد على التعريف الخاص، باعتماد على كلمة المرور خلال عملية الدخول الى نظام المعلوماتي

للجامعة، إضافة الى التدريب والتأهيل و التوعية بمخاطر الالكترونية وطرق موجهتها والإجراءات المساعدة على ذلك. (موسى **2022**، **442**)

3.5.3.الحماية التقنية

تعتبر الحماية التقنية أساسية بنسبة للمؤسسة الجامعية، وهذا يفرض عليها ان تشمل الحماية كل من النظام المعلوماتي والعاملين عليه من خلال الكشف، وإزالة كل البرمجيات الضارة والخبيثة ومحوها وهذا لكونها تهدد البيئة الافتراضية للمؤسسة الجامعية، من خلال الاعتماد على مكافحات الفيروسات التي تكون مضادة لكل فيروسات المنتشرة في الفضاء الإلكتروني ومن أشهرها Avira , Avast بإضافة الى هذا يستوجب تأمين منافذ الموجودة في الحواسيب والتي من خلالها يمكن توفير الأنترانت، من خلال الاعتماد على جدران النار التي تمنع وصول الفيروسات الخبيثة، عن طريق المنافذ المفتوحة كما ستوجب أيضا حماية سرية المعلومات التي بحوزة المؤسسة الجامعية، في مستودعاتها الرقمية والأرشيف من خلال الاعتماد على التشفير وكلمة السر التي تكون معرفة عند المرسل والمرسل اليه (رحموني، **2017**ص**444**).

وبهذا يمكن أن نعتبر أساس الحماية الوسط الجامعي، من الجريمة الإلكترونية وتقنيات الاختراق تفرض علينا التزام بتدابير الحماية والمواجهة من التنظيم، وحماية الخصوصيات مع دمج تقنيات الحماية من برامج وتطبيقات الحاسب الالي، التي يمكن من خلالها ابعاد الضرر وكشف عن الفيروسات الخبيثة وحذفها، مم يعود بالأمن على الحاسوب ونظام المعلوماتي وشبكة الأنترانت.

خلاصة الفصل

من خلال عرضنا للفصل السابق، يمكننا القول ان الجريمة الإلكترونية ظاهرة قائمة بذاتها وأصبح كل الأفراد والمؤسسات مثل الجامعة ومواردها البشري، من الأدريون والطلبة والهيئة التدريسية تحت تهديد وقوع ضحايا للهذه الجريمة التي أصبح ذات طابع عالمي ولا يستوجب أن يكون المجرم جزء من المحيط المؤسسة الجامعة، او قرب أفرادها حتى يرتكب جريمته وهذا راجع، لتطور تقنيات الإلكترونية للأرتكابها حيت تمكن المجرم من اختراق اي مستخدم للأنترانت يستهدفه في أي مكان وفي أي زمان نتيجة لترابط بين منظومات المعلوماتية العالمية وتشابكها إضافة امتلكها العديد من المميزات، التي تجعل منها صعبة الترصد من طرف المستخدم وضعف الأنظمة الأمنية و سرعتها الفائقة، والدقة في إصابة الهدف وهذا يرجع لمستوي خبرة المجرم في مجال البرمجة وتعامل مع التقنية و جودة حاسوبه الشخصي وقوة معالجه كمأن سرعة تدفق الأنترانت، تلعب دور كبير في عملية الاختراق حيث كلما كانت سرعة التدفق

أكبر كأنت عملية الاختراق سريعة وخطيرة على المؤسسة التعلمية اما الوسط الجامعي، والجامعة كمؤسسة تبقي المكون الأول للمورد البشري في الدولة الجزائرية، ويستوجب علينا دائما على تحقيق امنها من خلال اتخاذ تدابير للزمة للحماية الوسط الجامعي من الجريمة الإلكترونية، للكل من موردها البشري والبنية الرقمية خاصة بها، وفي الأخير تطرقنا في هذا الفصل إلى تبيين ماهية الجريمة الإلكترونية والوسط الجامعي الجزائري.

الفصل الثالث:

الوعي السيبراني في الوسط الجامعي الجزائري

III. الفصل الثالث: الوعي السيبراني في الوسط الجامعي الجزائري

1 التحول الرقمي في الوسط الجامعي الجزائري

1.1 الرقمنة في التعليم العالي.

2.1 مفهوم التعليم الإلكترونية

3.1 أنواع التعليم الإلكترونية

4.1 أدوات التعليم الإلكترونية

5.1 الهوية الرقمية للمؤسسة الجامعية وأفرادها

6.1 جهود الجامعات الجزائرية في التحول الرقمي

2 ماهية الأمن السيبراني

1.2 مفهوم الأمن السيبراني

2.2 أهداف الأمن السيبراني

3.2 شروط تطبيق الأمن السيبراني في الوسط الجامعي

4.2 نظريات الأمن السيبراني

5.2 أهمية الأمن السيبراني

3 الوعي السيبراني للجريمة الإلكترونية في الوسط الجامعي الجزائري

1.3 مفهوم الوعي السيبراني

2.3 مفهوم الوعي بالجريمة الإلكترونية.

3.3 إدارة الأمن السيبراني والتوعية السيبرانية في الوسط الجامعي

4.3 أهداف تقيم الوعي السيبراني في الوسط الجامعي

5.3 المؤسسات التنشئة الاجتماعية ودورها في تنمية الوعي السيبراني

تمهيد

يشهد العالم اليوم تطور لم يسبق له من قبل في المجال التكنلوجي الذي أثر على تحول بنية المؤسسة التعليم العالي والبحث العلمي في الجزائر، من البنية المادية الى البنية الافتراضية، وتغير في نظام التعليم من الحضوري الى التعليم عن بعد وحتى في جانب تقديم خدماتها الإدارية التي أصبحت من خلال البوابات الرقمية لتسهيل كل الوظائف وتقديم أحسن الخدمات وهذا نتيجة الاعتماد على شبكة المعلومات والحسابية في ذالك، حيث أصبحت الجامعة الجزائرية على مرحلة جديدة فما يخص تحقيق أمنها السيبراني من خلال، الاهتمام بتوفير الحماية للمعلومات المتوفرة في الأنترانت والمستودعات الرقمية للجامعة وبنية النظام الرقمي الخاص بها ومواردها البشري، للآن تحقيق الأمن الشامل في الوسط الجامعي يستوجب الاعتماد على الجانب التقني من برامج وأجهزة.... الخ، ومن الجانب الثاني هو المورد البشري فمن خلال تنمية وعيه السيبراني وتطوير مهاراته في استخدام الأمن للوسائط الإلكترونية كمأن هذا، الفصل الذي جاء تحت عنوان " الوعي السيبراني في الوسط الجامعي الجزائري" سوف يتم التركيز على ثلاث عناصر أساسية يتم من خلاله تعريف القارئ على التحول الرقمي في الوسط الجامعي الجزائري، من خلال التعريف بمفهوم التحول الرقمي والتعليم الإلكتروني وتحديد أنواعه وأدواته أضافة الى الهوية الرقمية للمؤسسة الجامعية وأفرادها التي تمنحها المرئية على مستوي العالمي، وتركيز على جهود الجامعات الجزائرية ووزارة التعليم العالي نحو التحول الرقمي اما فيما يخص ماهية الأمن السيبراني، بحكم مجال له ارتباط مع العالم الافتراضي حيث يتم الاشارة الى مفهومه وأهدافه وأهميته بإضافة الى شروط تطبيقه في الجامعة وتحديد النظريات الخاص به أضافة الى، الوعي السيبراني للجريمة الإلكترونية من حيث مفهوم الوعي بالجريمة المعلوماتية، كظاهرة والوعي السيبراني كمجال وتحديد كيفية إدارة الأمن السيبراني داخل الحرم الجامعي، وأهداف التقييم للوعي السيبراني ودور المؤسسات التنشئة الاجتماعية في تنميته.

1.التحول الرقمي في الوسط الجامعي الجزائري

1.1. الرقمنة في التعليم العالي

أصبح التعليم العالي في الوقت الراهن يواجه تحديات عديدة على جميع الأصعدة (المحلية والدولية)، ما يستدعي البحث عن الوسائل ذات الكفاءة العليا لتحقيق الأهداف التعليمية وجعل الباحث

الأكاديمي أكثر حيوية داخل المؤسسة الجامعية. تعتبر الوسيلة أداة كفيلة وقادرة على توجيه السلوك الفردي وتنظيمه.

تشير وثيقة "استراتيجية الجزائر الإلكترونية 2013" إلى أهمية وضع وتنفيذ سياسات قوية لتعزيز نمو الاقتصاد الرقمي في الدول المتقدمة. تؤكد الوثيقة أن تحقيق ذلك يتطلب وجود جمهور ملتزم ومتطلع إلى التطور، ويمكن تحقيق ذلك من خلال تقديم دعم قوي لصناعة تكنولوجيا المعلومات والاتصالات. كما تشدد الوثيقة على أهمية وضع خطة واضحة ومتماسكة تجسد مبادئ مجتمع المعلومات، وتشمل هذه الاستراتيجية الاقتصاد الحقيقي والمجال الرقمي. ويجب ملاحظة أن هذه الاستراتيجية صيغت في عام 2008 وكان من المقرر تنفيذها على مدى خمس سنوات، حيث تم تحديد فترة زمنية قدرها سنتان كنقطة مرجعية (أحميداتو، **2020**، ص **228**).

أما من حيث مفهوم الرقمنة، فهو من المفاهيم الواسعة. ووفقًا لتعريف تايلور (2007) فإن الرقمنة "تعني الفرق بين البتات (BTTS)، حيث يمثل البت كل ما له حجم ولون ويمكنه السفر بسرعة الضوء. وبالتالي، فإن الرقمنة تمثل نظامًا علميًا يتيح لبعض الأجهزة التقاط صور المواد المطبوعة، وتحويلها إلى لغة مشفرة، ثم تخزينها ونقلها واسترجاعها ونسخها وحتى تعديلها" (نجلاء، **2014**، ص **16**).

بالإضافة إلى ذلك، أصبحت جودة التعليم والتكوين الأكاديمي العالي على المستوى العالمي تفرض التكنولوجيا كتقنية جديدة شهدها المجتمع في جميع المجالات، خاصة في المجال العلمي الذي يعتبر الأساس في تطوير المورد البشري ومؤسساته. تعرف سناء إبراهيم أبودوقة (2013) جودة التعليم العالي بأنها "أسلوب لوصف جميع الأنظمة والموارد والمعلومات المستخدمة من قبل الجامعات ومعاهد التعليم العالي للحفاظ على مستوى المعايير والجودة وتحسينها" (إبراهيم أبودوقة، **2013**).

في هذا السياق، تجد الدولة الجزائرية نفسها اليوم في عالم يستخدم العولمة، مما يستوجب عليها الوعي بالمهام المنوطة بمؤسساتها التربوية والتعليمية، ومنها الجامعات على المستويين الداخلي والخارجي. يجب عليها التنظيم والتجريب لضمان التطور والتحكم في العلم والمعرفة، وتسجيل حضورها على المستوى العالمي من خلال بناء علاقات مع مؤسسات ومخابر علمية متطورة وتشجيع التبادلات الطلابية والنشر العلمي، مما يعود بتطوير برامج هذا النظام التعليم العالي وتحسينه.

حسب دراسة محمد يدو (2018)، فإن للرقمنة أهمية كبيرة في جودة التعليم من خلال:

- ضبط وتطوير النظام الإداري في المؤسسة التعليمية.

- الارتقاء بمستوى الطلاب في جميع المستويات.
- زيادة الكفاءة التعليمية ومستوى الأداء للفاعلين في الجامعة (يدو، **2018**، ص **267**).

باعتبار الجامعة مؤسسة إنتاجية تعمل على إثراء المعارف وتطوير التقنيات وتهيئة الكفاءات، مستفيدة من التراكم العلمي الإنساني في مختلف المجالات العلمية، الإدارية، والتقنية، فهي المؤسسة الأولى المكلفة بمناقشة القضايا الاجتماعية في جميع المجالات من خلال البحث الميداني والتحليل النظري. يلاحظ كل باحث أكاديمي أن الواقع قد عرف تغيرات سريعة بفضل العولمة، حيث أصبحت البنية الاجتماعية لا تتقيد بالحدود السياسية للدولة، مما يفرض على الجامعة ووسطها مواكبة التطور الاجتماعي، مما يؤهلها لتفسير القضايا الراهنة والرقي بها. لضمان جودة التعليم، حسب دراسة عائشة سلمة كيحلي وآخرين (2017)، يجب تحقيق الأبعاد الخمسة التالية:

الكفاءة أو الجدارة: انتقاء الطالب للمؤسسات التعليمية التي توفر له الخدمات والمميزات بشكل كافٍ وملائم، وتتميز هذه المؤسسات عن غيرها في طرحها وتقديمها للخدمات التعليمية.

- **الاعتمادية:** ينبغي أن تقدم مؤسسة التعليم العالي خدماتها التعليمية بصورة تعكس درجة عالية من الاعتمادية.
- **التعامل:** يجب أن يسود في المؤسسة التعليمية جو من الاحترام المتبادل والتعامل اللائق.
- **الاستجابة:** يركز هذا البعد على تحقيق الاستجابة العالية والسريعة للتغيرات في بيئة المؤسسات التعليمية (مؤسسات التعليم العالي).
- **فهم الطالب:** لتحقيق هذا البعد ضمن أبعاد جودة التعليم الجامعي، يجب التركيز على فهم الطالب الجامعي وإدراك حاجاته التعليمية (كيحلي، **2017**، ص **33**).

من خلال هذا، لضمان جودة التعليم العالي في ظل الرقمنة، يجب على الجهات الوصية، مثل وزارة التعليم العالي والبحث العلمي والحكومة، أن تحدد استراتيجية وأسلوبًا لوصف جميع الأنظمة والموارد والمعلومات المستخدمة من الجامعات والمعاهد التعليم العالي. يجب انتهاج معايير تتماشى مع مؤشرات الجودة ومؤشر الفرص العالمي، من خلال تنويع طرق التعليم الرقمي وتشجيع التفاعل مع المعلومات إلكترونيًا، وتصميم بيئة رقمية تسهل عملية الاتصال بين الطالب والجامعة، مما يعود بالإيجاب على جودة الحياة الرقمية للأكاديميين.

2.1. مفهوم التعليم الإلكترونية

يعتبر التعلم ظاهرة معقدة كونه جزءًا أساسيًا في بناء المعرفة للمجتمع. يعود ذلك إلى تغير أساليبه وطرقه ومناهجه بتغير المجتمع. يرى كل من Vedenpää وLonka (2014) أن "التعلم هو ظاهرة معقدة نتيجة لتحول البحوث في مجال التعلم من دراسة الأفراد الذين يكتسبون المعرفة والذكاء ككيانات ثابتة، إلى تسليط الضوء على جوانب التعلم النشطة والبنائية والتعاونية، في النهج الاجتماعي والثقافي للتعلم". حيث ينظر إليه على أنه جزء من العمليات الاجتماعية لبناء المعرفة بوساطة الأدوات والمعايير الثقافية (**Vedenpää & Lonka, 2014**, ص **1822**).

في المقابل، يشير كل من Tursunalievich وRahmat (2021) إلى أن مفهوم التعليم الإلكتروني هو مفهوم جديد نشأ مع ظهور تكنولوجيا المعلومات والاتصال. هذه التكنولوجيا أثرت بشكل كبير على الأوساط الأكاديمية والأفراد الفاعلين فيها من طلبة وهيئات تدريسية وجامعات كمؤسسات، مما أدى إلى ظهور مفاهيم جديدة مثل المجتمع الرقمي الأكاديمي والثقافة الرقمية (**Tursunalievich & Rahmat, 2021**, ص **248**).

التعليم الإلكتروني هو طريقة جديدة ومبتكرة تعتمد على الأدوات والتقنيات الرقمية في العملية التعليمية، مما يعزز من المرونة والسرعة في التواصل بين الطالب والأستاذ. يتم ذلك من خلال شبكة الإنترنت والتفاعل بواسطة الوسائط الإلكترونية المكونة من الحاسوب والشبكة الإلكترونية، والتي يتم عبرها تحويل المادة العلمية بكل صيغها إلى صور، أو فيديوهات، أو مستندات.

تم تقديم عدة تعريفات للتعليم الإلكتروني، حيث ترى د. خديجة بنطالب (2022) أن التعليم الإلكتروني هو "التعليم الذي يتم تقديمه عبر وسائل الاتصال الحديثة مثل الكمبيوتر والهواتف النقالة، أو أي وسيلة أخرى متعددة الوسائط التي تعتمد على الإنترنت بجميع أشكالها لنقل المعلومة للمتعلم عبر المحاضرات، والدروس، والمناقشات، والتمارين، والاختبارات، بهدف دعم وتسهيل عمليات التعلم في أي وقت وفي أي مكان" (بنطالب، **2022**، ص **3**).

في الختام، نستنتج أن نواتج الثورة التكنولوجية الرقمية التي شهدها الوسط الجامعي قد أدت إلى ظهور "المجتمع الرقمي الأكاديمي"، الذي يتميز بالمرونة والسرعة في تدفق المعلومات والتفاعل معها عبر الشبكات العالمية، بالإضافة إلى الاستخدام الآلي في إنجاز الأنشطة العلمية. من الخصائص التي تميز هذا المجتمع هي الإبداعية والتآلفية الموجهة لتحقيق الأهداف التعليمية.

3.1 .أنواع التعليم الإلكترونية

لقد طورت الرقمنة التعليم من خلال التوجه "نحو التعليم المفتوح، المكمل لتدريس التقليدي حيث أصبحت وسيلة فعالة في نشر المعرفة على نطاق واسع، تسمح لفئات عديدة من المجتمع لتفاعل مع معلومة وهذا النمط جديد من التعليم يتجسد في نوعين اساسيين:

1.3.1. التعليم عن بعد: يعرفه Picciano (2017) على أنه نموذج جديد في التعليم يعتمد على الأنترانت لبناء ونقل المعرفة وتحقيق التعلم التعاوني ويتميز بعديد من الخصائص أبرزها انه:

- تنوع الآراء في مجال العلم والمعرفة
- يسهل عملية التعلم حيث يوفر معلومات أكثر للمتعلم عكس الطريقة الكلاسيكية.
- يعتمد على التقنية دون حاجة الى المرد البشري وحضوره (**Picciano, 2017, p. 175**)

وقد برز كثير هذا نوع من التعليم خاصة في فترة انتشار وباء كرونة COVID-19 حيث يسهل للطالب والأستاذ من التعليم والتعلم، بإضافة الى التقييم وكل هذا يكون في الواقع الافتراضي حيث يتم تقديم المحتوي العلمي متمثل في الصور وصوت والفيديو للطالب عبر وحدات الإدخال الرقمية باعتماد الحاسوب والوسائط المتعددة، للعملية التدريس وتحقيق التفاعل بين المجوعة الطلابية في بيئة افتراضية لا تتقيد بالمكان والزمان. (**Collis & Smith, n.d., p. 2 ; Watermeyer et al., 2021, p. 624**)

2.3.1. التعليم الذاتي: هو نموذج جديد من التعليم يركز على تنمية المعرفة والمهارات الطالب باستعمال الأنترانت، حيث يري Zakhro Umarova (2020) " ان التعلم الذاتي مرتبط ارتباطًا وثيقًا بالتعليم. لذا، يجب أن ينظر إلى التعلم الذاتي في المؤسسات التعليمية العالية ليس كبديل للتعليم التقليدي، ولكن كإضافة إليه "(**Umarova, 2020, p. 6**)

كما يسمح للفرد، باكتساب معارف حسب اهتماماته العلمية ويمكنه هذا من تطوير ذاته ومن مميزات هذا نوع من التعليم هو المرونة والانماء والثقة وهذه الخصائص يجب ان يتحلى بها الطالب لباحث من خلال التحفيز وتخطيط والالتزام، حتي نكون نتائج التعلم فعالة فهنالك عديد من الدوارات والمساقات التدريبة والتعلمية التي يتم الإعلان عنها على منصات التعلمية مثلcoursera، khanacademy ،openLearning، حيث تعرف هذه المنصات تفاعل على نطاق واسع، بحكم تنوع مجالاتها بإضافة انها تمنح شهادات من جامعات معروفة عالميا ومعترف بها يمكن للفرد اضافها في سيرته الذاتية للإثبات كفاءته.

ومن خلال، مأتم ذكره سابق يمكن ان نعتبر دمج الرقمة مع التعليم قد كان له أثر اجابي على التعليم من خلال تنوعه وسهولة التعلم بنسبة للفرد، حيث انه أصبح لا يتقيد بالمكان والزمان فالبيئة

الافتراضية، قد سهل عملية تفاعل الطلاب مع المعلومة من خلال التعلم عن بعد والتعليم الذاتي وأصبح كل الافراد متساوون في امتلاك المعلومة بفضل الأنترانت.

4.1. أدوات التعليم الإلكترونية

باعتبار التعليم الالكتروني منظومة تفاعلية ترتبط بالعملية التعلمية، وتعتمد على البيئة الافتراضية في عرض المادة العلمية (من مقررات، أنشطة علمية، دروس، محاضرات.....الخ) يشترط عليها توفير العديد من الأدوات لتسهيل عملية التعلم، فكل من الحاسوب والأنترانت هم عناصر أساسية لربط العلاقة مع البيئة الافتراضية.

حيث عرفته أمل محمد عبد الله البدو (2021) كل من التعليم عن بعد والمنصات التعليمة، التي يعتمد عليها بأنها "البيئات التي تحاكي بيئة التعليم المادية التقليدية من حيث مكوناتها ووظائفها وتتميز هذه البيئات بأنها بسيطة في استخدامها وسهولة الدخول إليها" تتواجد هذه البيئات على مواقع محددة على الإنترنت، كما تعرف الباحثة المنصة التعليمية بأنها بنية على برنامج داعم يهدف إلى صقل مهارات الطلاب المعرفية والإدراكية والتقنية في التعلم الذاتي والمستقل" (البدو، **2021**، صفحة **180**)

لكن هنالك مجموعة من الوسائط، التي يعتمد عليها الأستاذ في انجاز مهمته التعلمية عن بعد حيث تعرف هذه الأدوات، تنوع في الخدمة التي تقدمها للمستعمل لها حيث انا لكل نوع من هذه الأدوات خاصية تميزها، عن الأخرى لكن لم تجتمع وظائفها تشكل لنا محتوي علمي متعدد الصيغ.

فمن البرامج الواسعة النطاق من حيث الاستعمال في الوسط الأكاديمي نجد:

أ-برنامج: (PowerPoint) الذي يعتمد علية الأساتذة والباحثين في تقديم العروض خاصة بهم في المحاضرات، او الملتقيات الدولية حيث يدعم المحتوي علمي في صيغ متعددة على شكل صورة ورسوم متحركة (**Craig & Amernic, 2006**).

ب-خاصية : Secreen sharing يعرفها الباحث مايكل ستيفنسون(Michael Stevenson) وأخرون "نظامًا متكاملًا يتيح للمستخدمين "مشاركة شاشات أجهزة الكمبيوتر الخاصة بهم، أو النوافذ، أو مناطق الشاشة التي يرغبون فيها بشكل صريح مع بعضهم البعض،محاكيًا المشاركة عبر الكتف في استخدام الكمبيوتر"(**Stevenson et al., 2022, p. 771**)

ومن خلال هذا فأن مشاركة الشاشة من الحاسب الشخصي للأستاذ في شرح المادة العلمية كما تدمج وظائف اخري مثل بث الفيديو، الرسائل الفورية، استطلاعات الرأي عبر الإنترنت، التحرير في الوقت الفعلي، والتقاط الشاشة والأدوات المختلفة لتحليلات المتعلم تتيح لطالب سهولة في التفاعل مع الأستاذ ومشاركة آرائهم.

ت- white board: التعليم عن بعد لم يتخلى عن السبورة في عملية التعلمية الافتراضية بلا طورها في أداة تسمح لجميع الطلبة بالتفاعل الجماعي خلال الدردشة المرئية وتدعي هذه الأداة ب white board تعتبر برنامج يسمح بالكتابة والشرح عن بعد من خلال تقديم ملاحظات خلال محاضرة. حيث أجريت العديد من التجارب عليها فوجد ان من السهل التفكير في أن جميع المعلومات هي معلومات جيدة، مما يؤدي إلى زيادة عدد السبورات البيضاء لا يمكن اعتبار عرض المعلومات بهذه الطرق كأمر مثلى حيث أن تصفية المعلومات هي جزء مهم من نوع التحسين. **(F.Berglund et al., 2016, p. 1128)**

ث-تخزين المحتوي الرقمي التعليمي: في ظل توجه نحو التعليم عن بعد او كما يسميه الباحث ميلوراد ب. ستيفيتش(Milorad P. Stević) بالتعلم المتنقل حيث يري انه يستوجب نظم إدارة التعلم من خلال نشر نظام إدارة التعلم في عالم المحمول باستخدام خدمات الويب ومبادرات التوافق أو استيعاب تطبيقات التعلم المتنقل الخارجية في نظام إدارة التعلم.**(Stević, 2014, p. 60)**

ومن خلال هذا نستنتج ان فتخزين الوثائق في القديم كان يعتمد على الأرشيف الورقي اما مع البيئة الافتراضية قد سهلت عملية تخزين المحتوي الرقمي من خلال الاعتماد على البرامج المطورة من طرف شركة غوغل ومن أشهر هذه التطبيقات نجد كل من google drive و One Driveالاكثر استعمالا فهي عبارة عن مجموعة من برامج والتطبيقات التي تخزن المحتوي الرقمي بمساحة ذاكرة كبيرة تسهل عملية مشاركة المعلومة الرقمية بين الطلبة.

ج-منصات التحاضر عن بعد: نتيجة لظروف الوباء (Covid-19) التي مرى عليها العالم أجريت العديد من التجارب فيما يخص التعليم من خلال التحاضر عن بعد حيث "يتيح هذا للطلاب التعلم بوتيرتهم الخاصة" كما تم تطوير عديد من المنصات الرقمية لتكون بديلة للقاعات الدراسية حيث ان التفاعل في القديم كان بشرط حضور كل من الطالب والأستاذ في مكان واحد حتي تتم عملية التعلم لكن مع المنصات الرقمية ومن بينها Zoom و google meet تسمح للمستعملها، الاتصال عن طريق الصوت والصورة عن طريق الحاسوب او الهاتف كما تسمح بفتح عيديد من الغرف الافتراضية وتقسيم الطلبة الى

أفواج وتسهل تسجيل الطلبة الحاضرين والغائبين عن الحصة الدراسية في نفس السياق تسهل عملية مراقبة لجميع الغرف الافتراضية وتتبع سير الدرس (Cuschieri & Calleja Agius, 2020, p. 675)

ومن خلال هذا يمكن ان نعتبر انا البيئة الرقمية التعلمية هي هيكل منظم يجمع، بين عديد من العناصر الأساسية لصناعة ومشاركة محتوي العلمي رقميا من خلال اعماد على العديد من الأدوات، من بينها الحاسوب وشبكة الأنترانت بإضافة الى الوسائط المتعددة المدمجة، مع الرقمنة لتسهيل عملية مشاركة المادة التعلمية مع الطلبة وهذه أبرز التحولات الرقمية التي شهدها الوسط الجامعي.

5.1.الهوية الرقمية للمؤسسة الجامعية و أفرادها

لقد كان لتفاعل تكنولوجيات الاعلام والاتصال، مع المؤسسة الجامعية ومواردها البشري أثر على عملية التفاعل مع مكونات هيكلها التنظيمي، فتصنيفها على مستوي عالمي في ضل الترابط الشبكي عبر الأنترانت، فرض على المؤسسات التعليم العالي بناء هوية رقمية التي تسمح لها بجلب متفاعلين رقمين على نطاق واسع.

فالهوية الرقمية حسب طلحة مسعودة (2020) تعتبر مجموعة من السمات تعرف بها المؤسسات، عن نفسها على نطاق العالمي وهي عملية محاكاة الهوية داخل نظام رقمي تسمي "بالهوية الرقمية" ومن خلالها يتمكن العملاء من طلبة واساتذة، الاطلاع عليها وعلى تخصصاتها العلمية وخدماتها الرقمية المقدمة وطرق التواصل بها وتسجيل بها وتحديد موقعها الجغرافي في الخارطة الافتراضية، بإضافة الى مجلاتها ومخرجاتها العلمية من مقالات العلمية ومذكرات تخرج وملتقياتها العلمية التي احتضنتها (طلحة،2020ص136).

فالهوية الرقمية للمؤسسة، هي مرحلة انتقالية للبنية التحتية خاصة بها من بنية اجتماعية الى بنية الوسائط المتعددة حيث ساهم، هذا التحول على تغير جذري في مفاهيم الوسط والهيكل التنظيمي للجامعة، وظهور عديد من المفاهيم الجديدة التي تعتبر مكونات الجامعة الرقمية، ومن بينها الإدارة الرقمية والمكتبة الرقمية والمستودع الرقمي والبريد الالكتروني والموقع الالكتروني وتعتبر من الملحقات الأساسية لها التي يجب التعريف بها.

فبداية التحول الرقمي الذي شهدته الجامعة كان من خلال تصميم موقع الكتروني الذي يعرف على انه مجموعة من الملفات والموارد ذات الصلة التي يمكن وصول اليها عبر شبكة الويب عن طريق الرابط الالكترونية، اما بنسبة للإدارة العمل داخل الجامعة كان من خلال انشاء الإدارة والمكتبة الرقمية، حيث

اصبح العمل ومتابعته تتم عبر استخدام برامج مخصصة في الحاسوب واستعانة بعديد من وسائل التواصل مثل البريد الالكتروني حيث يتطلب من العامل ان يمتلك حاسوب و يكون ملم بمهارات الإدارة الرقمية وقواعدها، اما المكتبة الجامعية وكل ما تحتويه من كتب ومراجع أصبحت عبارة عن موارد مخزنة بصيغة رقمية يتم الوصول اليها افتراضيا من خلال موقع الالكتروني خاص بمستودع الرقمي للجامعة الذي يحتوي على جميع الإنتاجات المعرفية والعلمية للجامعة.

وتأخذ الهوية الرقمية للمؤسسة عديد من الأشكال، بحكم إعادة بناء نفس الهياكل المادية للمؤسسة بصيغة جديدة من خلال نقلها الى الواقع الافتراضي، وهذا يدخل في أطار الجامعة المفتوحة حيث يتسنى للجميع التواصل مع جامعة اما حضوريا او عن بعد وذلك من خلال تقديم خدمات الرقمية ومن بين الهيكل الرقمية للمؤسسة الجامعية هي:

1.5.1.الإدارة الرقمية: يشير مفهوم الإدارة الإلكترونية إلى عملية تحويل جميع مهام وأنشطة المؤسسة الإدارية إلى عمليات مؤتمتة، باستخدام التقنيات والأدوات المعلوماتية المناسبة، بهدف تحقيق أهداف الإدارة الحديثة، إنها مجموعة من العمليات التنظيمية التي تربط المستفيدون ومصادر المعلومات بواسطة وسائل الاتصال الإلكترونية، بهدف تحقيق أهداف المؤسسة في التخطيط والإنتاج والتشغيل والمتابعة والتطوير.(رزقي & حسين, **2023**, ص**109**)

ونستنج انها نموذج جديد للإدارة الكلاسيكية، حيث تعتمد الإدارة الرقمية على التكنلوجيا الحديثة المدمجة مع الأنترانت وأجهزة الحاسوب والبرامج للإدارة المهام الموكلة للموظفين الإدارة، وهي تعتبر منظومة تعتمد على النمط الالكتروني في تعزيز التواصل بين الطلبة والإدارة وفرق العمل داخل الجامعة، كما تسهل عملية التواصل بين مؤسسات الجامعية على المستوي الوطني والعالمي.

2.5.1.المكتبة الرقمية: مجموعة من الوصلات، أي البيانات ذات الصيغة الرقمية القائمة على شبكة الإنترنت بدلاً من إدارة الموارد نفسها أي الكتب والمراجع الورقية، حيث عرفت كل رحاب فايز احمد سيد وعمر حوتية(2020) المكتبة الرقمية تُعرف بأنها "المكتبة التي تحتوي على مصادر معلومات رقمية، سواء كانت مصادر أصلية تم إنتاجها بشكل رقمي أو تم تحويلها إلى صيغة رقمية، وتتم عمليات تنظيمها وإدارتها باستخدام نظام آلي، ويتم الوصول إليها عن طريق شبكة الحواسيب، سواء كانت محلية أو موسعة أو عبر الإنترنت (ف.رحاب, ع حوتية، ص**2020**)

3.5.1.المستودع الرقمي: يشار عادةً إلى قاعدة البيانات على الإنترنت للأعمال العلمية التي يديرها الباحثون باسم "الأرشيف المفتوح". يعتبر هذا الأرشيف قاعدة بيانات تديرها الباحثون أنفسهم، ويجعلون فيها أعمالهم العلمية قابلة للبحث والاطلاع عليها. يُعرف مصطلح "الأرشيف المفتوح" كمستودع للأعمال الفكرية، وقد قامت أمل محمد أحمد حسن المغربي (2022) بتعريفه كالتالي: "المستودعات هي التابعة للجامعات والمؤسسات والمعاهد والنظم البحثية والتعليمية، تهدف هذه المستودعات إلى جمع معظم أو جميع الإنتاج الفكري للباحثين المنتسبين إليها في مختلف المجالات أو في عدد من المجالات، أو في مجال واحد وفقًا للتغطية المخططة للمستودع، وتسعى أيضًا لتوفير هذا الإنتاج للمستفيدين سواء داخل المؤسسة أو خارجها، وذلك وفقًا للسياسة التي يقررها المسؤولون عن المستودع" (محمد أحمد حسن المغربي، **2022**، ص **300**).

اما بنسبة للباحث الأكاديمي فالرقمنة، كان لها أثر بليغ عليه حيث وفرت له عديد من المنصات الالكترونية التي يتمكن من خلالها بناء هوية رقمية خاصة به، يتم من خلالها رفع بيناته الشخصية وتخصص العلمي واهتماماته العلمية.

بإضافة الى ذلك مهارته ومؤهلاته العلمية وابحاثه المنجزة، او التي سوف ينجزها مستقبلا فهناك عدة أنواع من المنصات الرقمية، ومواقع الويب المطورة خصصت له أشهرها هي موقع التوصل الاجتماعية، مثل فيسبوك وتويترو لنكاد حيث تمكنه من تسهيل عملية الاتصال البشري، على نطاق واسع باعتبارها منظومة من الشبكات الالكترونية، تتيح للباحث الأكاديمي انشاء موقع خاص به في البيئة الافتراضية وبناء، علاقات مع مجموعة من الباحثين تشاركه نفس الاهتمام.

اما بنسبة لنوع الثاني، من مواقع الويب المطورة وهي خاص بمجالات البحث العلمي فقط حيث تمنح الباحث مجموعة من الاحصائيات الخاصة بالمنتوج العلمي خاص به المنشور على قاعدات البيانية والمجالات العلمية، تمنحه إحصائيات لعدد الاقتباسات و الاستشهاد بأبحاثه من طرف بحثين اخرين ومن اشهرها (Google Scholar و ResearchGate و...Academia.edu)يتم من خلال هذه المنصات فهرس العمل البحثي خاص بالباحث.

ومن خلال هذا فالهوية الرقمية قد غيرت من بيئة المؤسسة والفرد حيث سهلت عليهم عملية الترويج والاشهار للأبحاث العلمية، وبناء هوية رقمية تسهل لهم العمل الإداري بنسبة للمؤسسة الجامعة ومواردها البشري كمان للباحث كان له نصيب من الأثر حيث منحت له العديد من المواقع الويب المطورة في مجال البحث العلمي التي توفر مقروئية على نطاق واسع للأبحاث.

6.1. جهود الجامعات الجزائرية في التحول الرقمي

تضع وزارة التعليم العالي والبحث العلمي الجزائرية، العديد من المشاريع في إطار رقمنة الجامعة لتكون وحدة لها كيانها المستقل، من الناحية الفنية والمالية والإدارية وهذا لتسهيل عملها وتيسير اجرأت التحول الرقمي لها، مما يجعل كل جامعة الدولة الجزائرية في تكامل رقمي، مع بعضها البعض ويدخل هذا في إطار دعم مراكز المعلومات لتعليم العالي ووضع أليات، التي تضمن التكامل بين جميع تطبيقات نظام المعلوماتي للاتصال للجامعة الجزائرية ومن بين المشاريع الرقمية التي شهدتها الجامعة الجزائري هي:

1.6.1. مشروع التعليم عن بعد: يحتل التعليم عن بعد مكانة هامة في المنظومة التعليمية في قطاع التعليم العالي، وهو أحد طرق التعليم الحديثة الذي يقوم على وجود المتعلم في مكان يختلف عن المصدر الذي يكون الكتاب أو المعلم أو حتى مجموعة الدارسين (لالوش، **2021**ص**130**).

حيث يهدف هذا المشروع الى توفير بيئة تعليمية مرنة، بها إستراتيجيات تعتمد على استخدام أساليب التدريس بشكل حديث كما تساهم في دعم القرارات، وسرعة إنجاز المعاملات الإدارية والاستغلال، الأمثل للبيئة التحتية المرتبطة بالأنترانت بنسبة للمؤسسة الجامعية حيث توفر سهولة، في التوصل بين أطراف العملية التعليمية عبر المنتديات والبريد الإلكتروني دون حاجز للوقت والمكان (على كاعوه،**2020** ص**140**).

وقصد إضفاء انسجام على الهياكل المؤسسة الجامعة والتكنولوجية المستعملة ووسائلها وتقنياتها البيداغوجية، أوصت وزارة التعليم العالي والبحث العلمي، باعتماد فضاء رقمي موحد، متمثلا في أرضية مودل MOODELE في عمليتي تصميم الدعائم، الموجهة للتعلم عبر الخط ووضعها حيّز الخدمة و تعتبر مشروع التعليم، من مشاريع التي شهدته الجزائر حديثا وخاصة في الفترة الوبائية التي مرى بيها العالم (زايد، **2022**).

2.6.1.منصة بروغراس: بغرض تطوير أداء الإدارة الجامعية، وتحقيق الكفاية في استخدام الموارد والتوزيع الأفضل لها، وتأدية أنشطتها سواء كانت تعليمية الإدارية، خاصة في ظل نظام ال أم دي، الذي يتميز بكثرة التخصصات والتدرجات العلمية من سنة لأخرى طبقت وزارة التعليم العالي والبحث العلمي ،أنظمة معلوماتية إلكتروني كان الهدف الرئيسي منه هو تبسيط الولوج إلى المرفق العمومي ورقمتنه، إضافة إلى تتبع مسار الطلبة في ظل نظام ال أم دي ،والتحكم بكل المعطيات التي تسير الجامعة وهذا الهدف ذو بعد استراتيجي استشرافي لاتخاذ القرار (طواهيروأخرون،**2021** ص**40**).

كما أن هذا، النظام يتميز بالإنصاف والشفافية حيث انه يمكن الطالب الجامعي من التسجيل في أي عرض من عروض الماستر والدكتوراه، ويمكنه من الاطلاع على النتائج بكل وضوح وشفافية، تعتبر هذه المنصة نظام معلوماتي يمكن من تسيير شامل لكل شؤون الجامعة، ويظهر هذا على سبيل المثال لا الحصر في:

تسجيل الطلبة الجدد وتوجيههم وتحويلهم، منح الطالب حساب يتبعه طيلة مساره الدراسي ويطلعه كل أموره البيداغوجية.

- حفظ شامل لمسار الطالب الدراسي.
- صياغة برامج التوزيع الزمني والحجم الساعي للأساتذة.
- تسيير عملية المداولات.
- تسجيل في توظيف وتوظيف بنسبة للأساتذة التعليم العالي.

وتعول الجامعة الجزائرية، على أن تكون هذه المنصة نظام معلوماتي شامل يوفر قاعدة معطيات متكاملة عن الطلبة والأساتذة.

3.6.1. البوابات الرقمية: البوابة الإلكترونية هي من المشاريع، التي تعرف تنامي في المؤسسة التعليم العلي الجزائري الذي من خلالها يستطيع أي زائر للبوابة الإلكترونية، من داخل أو خارج الجامعة التعرف والاستفادة من الخدمات المقدمة على البوابة، كما يمكن من خلالها توظيف أفضل التقنيات والبرمجيات، المتوفرة لزيادة التعاون والتواصل بين مختلف الكليات بالجامعة وبين الجامعات بعضها بعضًا. (سدوس وبن السبتي، **2020**، ص **250**)

وتعمل وزارة التعليم العالي، بما يكفل الوصول إلى أعلى مستويات الأداء كما تساهم البوابات الرقمية، في ترقية النشر العلمي والمخرجات العلمية الخاصة بالمؤسسة العلمية ومن بين البوابات الرقمية في الجزائر نجد على النحو التالي:

- المنصة الجزائرية للمجلات العلمية Asjp.
- النظام الوطني لتوثيق عبر الأنترنات sndl
- البوابة الوطنية للأشعار عن الأطروحات .pnst
- مشاريع البحث التكويني prfu. البرامج الوطنية للبحث PNR

وتعتبر من أكثر البوابات التي تستعمل في الجامعات الجزائرية وذات ارتباط مع وزارة التعليم العالي والبحث العلمي، ومن خلال هذا يمكن القول إن للدولة جزائرية جهود مبذولة في عملية تحول الرقمي للمؤسسة التعلمية، من خلال العديد من المشاريع التي تدخل في اطارة انتقال من تعليم التقليدي الى التعليم المفتوح و تشجيع على التعليم عن بعد وتطوير الأداء الأدارة الجامعية من خلال المنصات والبوابات الرقمية.

2.ماهية الأمن السيبراني

1.2.مفهوم الأمن السيبراني

الأمن السيبراني، هو فرع من فروع الأمن الأنسان في ظل الثورة المعلوماتية والإلكترونية التي شهدها العالم، حيث يعد من المفاهيم الحديثة الذي جاء متزامن مع الرقمنة التي شهدتها المؤسسات الجامعية، بإضافة الى ذلاك أصبحت الجامعة والأفراد الفاعلين فيها من طلبة وأستاذة وعمال الأدراة، يعتمدون اعتمادا أساسيا على الأنترانت في عملية التواصل والتفاعل الافتراضي في مجال التعليمي، وتقديم الخدمات الرقمية من طرف الأدارة لهم عبر موقعها الإلكتروني، او من خلال البوابات الرقمية والمنصات الإلكترونية. (ماجد، **2021**، ص **278**).

كمأن مفهوم الأمن السيبراني يتعلق بانعدام الأمن، الناتج عن الممارسات أو العمليات عند استخدام الأنترانت لجعلها أكثر آمنة، ويشير إلى مجموعة من الأنشطة والتدابير، على حد سواء التقنية وغير تقنية ،التي تهدف إلى حماية البيئة الافتراضية الحيوية والبيانات التي تحتويها من جميع التهديدات المحتملة.(**Cavelty, 2010,p401**)

ويعرف الأمن السيبراني بأنه الأمن الذي يهتم بأمن الشبكات، والأنظمة المعلوماتية للمؤسسة الجامعية، بحكم أنها تعتمد على رقمنة هياكلها لتسهيل عملية التفاعل بين المؤسسة الجامعية وموردها البشري، وذلك عن طريق الأجهزة الحاسوبية المتصلة بالأنترانت فعملية اتصال تكون من خلال مشاركة البيانات الرقمية، التي تكون خاصة بها وتكون متعددة الصيغ من (مستندات وصور وفيديوهات..... الخ) (عوفي، **2022**، ص **113**).

وبناء على العديد من الأدبيات والدارسات السابقة التي كانت في مجال الأمن السيبراني قد أعطت عديد من التعريفات لمفهوم الأمن السيبراني حيث:

عرفه جبور(2016): "بأنه أمن الشبكات والأنظمة المعلوماتية والأجهزة المتصلة بالأنترانت" (جبور، **2016**، صفحة **25**)

كمعرفه كل من Canongia, C, & Mandarino(2014)على أنه فن وجود واستمرار المجتمع المعلوماتي من خلال ضمان وحماية المعلومات واصولها وبنيتها التحتية في الفضاء السيبراني" (**Canongia, C, & Mandarino, R., 2014, p. 24**)

ومن خلال ما تمت تقديمه من تعريف حول الأمن السيبراني، يمكن ان نعتبره مجموعة من الإجراءات التقنية والإدارية للجامعة، التي تشمل العمليات والأليات التي يتم اتخاذها لمنع أي تدخل او تسلل غير مصرح به لنظام الالكتروني، للجامعة لتجسس واختراق استخدام للمعلومات والبيانات الإلكترونية للجامعة الموجودة على نظام الاتصالات والمعلومات لضمان وتأمين وحماية وحفاظ على سرية البيانات الشخصية، للأساتذة والطلبة وحماية المعدات والتقنيات خاص بالجامعة من الإتلاف.

2.2.أهداف الأمن السيبراني

باعتبار ان الأمن السيبراني أساس للحماية البنية الرقمية، للمؤسسات الدولة تسعى الدولة الجزائرية الى حماية مؤسساتها التعليمية وخاصة المؤسسة التابعة لوزارة التعليم العالي والبحث العلمي، من جامعات ومعاهد التعليم وهذا بحكم ان على مستوي العالمي تشهد المؤسسات التكوين العالي عديد من الهجمات السيبرانية، على بيئتها الرقمية ونظامها المعلوماتي، وهذا راجع الى أهمية هذه المؤسسات في تطوير الدولة في شقها الاقتصادي والسياسي والاجتماعي والثقافي للأنها المكون الأول للمورد البشري ومن الأهداف الرئيسة التي يهدف تحقيقها من خلال الأمن السيبراني هي:

1.2.2. تحقيق الأمن للبيئة الافتراضية للجامعة

فبحكم دمج الرقمنة مع التعليم العالي وانتقال من تعليم المادي الى التعليم الافتراضي الذي يعتبر من الطرق الجديدة التي شهدتها المنظومة التعليمية الجزائرية، وخاصة مع الأزمة الصحية العالمية للوباء كرونة، لهذا أصبح يستوجب أكثر من السابق تعزيز الحماية أنظمة التقنيات التشغيلية للجامعة في كافة الأصعدة ومكوناتها، من أجهزة وبرمجيات بإضافة الى الخدمات الرقمية التي تقدمها الأدارة الجامعية والبيانات المخزنة في الحافظة الإلكترونية.

اضافة الى هذا توفير بيئة أمنة وموثوقة للتعاملات في الجامعة، أما من حيث عملية تفاعل بين الطلبة والأساتذة، في عملية مشاركة المحتوي العلمي اومن جانب تفاعلهم مع الأدارة الجامعية لتوفير

استمرار عمل الجامعة، وحفاظ على نظامها المعلوماتي بتأخاذ التدابير اللزمة لحماية المورد البشري للجامعة (الصانع وآخرون، 2020، ص 50).

2.2.2. أدارة المخاطر السيبرانية التي تستهدف الجامعة

ان هياكل الرقمية للجامعة، مثل الموقع الإلكتروني والمستودع والمكتبة الرقمية إضافة الى الأدارة وبواباتها الإلكترونية تدخل في إطار البنية الافتراضية للمؤسسة الجامعية التي تعرف اقبال كبير من المتفاعلين الرقمين، حيث تعتبر هذه البنية حساسة للهجمات الإلكترونية يستوجب توفير كل المتطلبات اللازمة للحد من المخاطر، والجرائم الإلكترونية التي تستهدف مستخدميها وهذا يكون من خلال إدارة المخاطر.

بإضافة الى هذا مقاومة البرمجيات الخبيثة التي تستهدف المستخدمين، والنظام المعلوماتي التي تأدي الى اضرار فمن خلال إدارة المخاطر السيبرانية، يتم الحد من التجسس والتخريب الذي تتعرض اليه الجامعة والأفراد الفاعلين فيها، وتخلص من نقاط الضعف في الأنظمة الحاسب الآلي والهواتف المحمولة، بمختلف أنواعها التي تكون مستهدفة من الهاكر، مما يعود بالحماية الشاملة على (الشبكات أنظمة التقنية المعلومات سرية وخصوصية البيانات الشخصية) التابعة للمؤسسة الجامعية (هبة هاشم، **2020**، ص **102**).

3.2.2. إدارة المحتوي الرقمي للجامعة

تتضمن برامج الأمن السيبراني وتتيح حماية خدمات، حفظ وتنظيم وبث المحتوي الرقمي على الحاسوب عن طريق الأنترانت، خلال عملية تعامل مع التقنيات والمعلومات في الجامعة من طرف المستخدمين من طلبة وأساتذة والعمل، على تنظيمها وادارتها وتحليل المخاطر التي تهددها او محتملة، من خلال الأعداد الجيد القائم على الفهم والأدراك وتحيد عناصر النظام والعمليات والمخاطر، ومن ثم تحديد المعايير التهديد ونطاق الحماية المطلوب منها (عزة ووأخرون، **2020**، ص **168**).

3.2. شروط تطبيق الأمن السيبراني في الوسط الجامعي

مع زيادة المخاطر السيبرانية التي تستهدف الجامعة، باعتبارها مؤسسة لتنمية المورد البشري وتكوين الكفاءة للدولة فيستوجب على السلطات المحلية الى حمايتها من خلال وضع خط استراتيجية، يتم من خلالها ضمان الأمن لنظام المعلوماتي ولفاعليتها يستوجب توفر عديد من الشروط الأساسية، التي من

خلالها يمكن من خلالها حفاظ على الأمن في البيئة الافتراضية التعليمية وإدارة المخاطرة التي توجهها وإدارة المحتوي الرقمي خاص بها وهي على النحول التالي:

1.3.2. مختصين في مجال الأمن السيبراني: يقصد بالمختصين هو العنصر البشري، المعني بإدارة الأمن السيبراني حيث بحكم كفاءته في مهامه المتعلقة بالمجال الأمن فدوره مثل دور الجندي كما يحتاج تدريبات دورية لتحديث معارفهم بحكم أن تقنيات التكنلوجية، تعرف تغير سريع لذلك يستوجب تحديث معرفة الأخصائي لمواكبة، تطور التكنلوجي وهذا ميساهم في امن الجامعة وبنيتها التحتي.

2.3.2. القيادي: ان عملية تحقيق الأمن السيبراني في الجامعة يستوجب قيادي للأدرة الذي يكون مسؤول على الفرق المكلفة بالأمن، على جميع مستويات الجامعة بحكمها مؤسسة فهيا لا ترتكز على فرقة الأمن داخل الجامعة لضمان أمنهم، فهو مفهوم خاطئ للآن الامن السيبراني هدف يتحقق من خلال عمل جماعي، يكون بين الإدارة الأمنية وكل المستخدمين للبيئة الافتراضي في الوسط الجامعي (الطاهر، **2021**، ص **64**).

3.3.2. تقنيات وأدوات ضمان الأمن: لبناء قدرة دفاع الكتروني جيدة وقوية يستوجب على الجامعة استخدام وسائل وتقنيات حديثة متعددة الميزات، التي تسهل كشف الدخيل على نظام المعلوماتي للجامعة ومواجهة التهديدات المكتشفة، والتهديدات المحتملة على المؤسسة الجامعية وحد من خطورتها.

4.3.2. الدعم المالي والتخطيط من الأدارة العليا لمؤسسة الجامعية: يستوجب على الجامعة السير بخطة منظمة لتحقيق أمنها، وذلك من خلال تقيم شامل للمؤسسة الجامعية ونظامها وتحديد اهم نقاط الضعف، فيها التي تستوجب دعم مالي ويشمل التخطيط المكونات المادية للمؤسسة مثل الحواسيب والوسائل التقنية، بإضافة الى المورد البشري الثي يعتبر الحلقة الأضعف لذلك فعملية تخطيط تجمع بين الوسائل الأمن والوعي بالأمن (أحمد وفتحي، **2020**، **454**).

4.2. نظريات الأمن السيبراني

تختلف المؤسسات حسب نظام عملها ومجال الذي تتخصص فيه فمن المؤسسات ذات طابع اقتصادي مثل البنوك والشركات والمؤسسات الاقتصادية الخاصة والعامة، منها ذات طابع عسكري وقانوني، مثل المؤسسات التابع للوزارة العدالة والدفاع أضافة الى الجامعة كمؤسسة الأساسية في أي دولة، ويستوجب تحقيق الأمان وإدارة المخاطر لهذه المؤسسات ومساعدتها في التخفيف من استغلال

البنية التحتية، ونظامها المعلوماتي نتيجة لتصميم النظام السيئ او اختراق من المجرمين الإلكترونيين (Gayness Clark et al., 2009, p. 8).

ولن يتم هذا الى من خلال فهم الألية وكيفية عمل المؤسسات، للإدارة ومعالجة المخاوف السيبرانية التي تواجههما، فالأنظمة دائما متكون لها ثغرات في بنيتها الرقمية ونظامها المعلوماتي، تجعلها عرضة لهجمات الكترونية تكون ببرامج متطورة تكون اما من متسللين على مستوي وطني او دولي، لذلك يستوجب دائما توفير لها حماية التقنية والبشرية من اخلال اعتماد على البرامج الحديثة، وأخصائيين كفء للحماية الأنظمة المعلوماتية خاصة بالمؤسسة(Guozhu et al., 2015, p. 15).

هنالك العديد من نظريات النظام المعلوماتي التي يمكن تطبيقها في مجال الأمن السيبراني لفهم وتفسير الظاهرة ومن بين هذه النظريات نجد كل من نظرية السلوك المخطط ونظرية الردع ونظرية التحفيز الحماية:

1.4.2. نظرية السلوك المخطط

تري نظرية السلوك المخطط انه يستوجب على المؤسسات تنفيذ وتوفير تدابير أمنية وقوية لتخفيف من الهجمات السيبرانية، على نظامها المعلوماتي ومواردها البشري، حيث غيابها يأدي بخطر على البنية الرقمية ونظام المعلوماتي، بنسبة للمؤسسة ويشكل هذا تهديدا للمورد البشري بطريقة مباشرة او غير مباشرة ومن مخرجات الأساسية للنظرية(Loukaka & Rahman, 2017, p. 16) هي:

أ-التحول الرقمي الذي شهدته المؤسسات نتيجة التطور التكنولوجي يفرض عليها اعتماد على أنظمة الأمن السيبراني، من خلال أستخدم جدران الحماية وبرامج مكافحة الفيروسات والنسخ الاحتياطي للبيانات والتحكم، في الوصول للقاعدة بيناتها بنسبة للعمال، وتفرض عليه أتباع كل خطوات الأمنية قبل دخول لواجه العمل وبهذا يحمي نفسه.

ب-إضافة الى، أتباع سياسة للأمن السيبراني للمؤسسة من خلال التطوير التقني واعتماد على برامج متطورة للحماية البنية الرقمية، والتركيز على تريب والتعليم بنسبة للموظف للآن كلما كان مستوي ادراك علي لتهديدات السيبرانية التي توجهه عند استخدام الأنترانت عند العمل كلما كانت نسبة المخاطر قليلة.

ت-دراسة العوامل التي تؤثر على الموظفين، يساهم في بناء المخطط الأمني التي تسير عليه المؤسسة في سياستها الأمنية، للآن ضبط العوامل المؤثر هو الحلقة أهم في تحليل وتفسير كل مشاكل التفاعل،

داخل تنظيم المؤسسة إضافة الى الحوار المتبادل بن كل أعضائها بشأن سياسات، الأمان التي يستوجب السير عليها باعتباره الحلقة الأضعف هو الموظف.

2.4.2. نظرية الردع

تري نظرية الردع ان السلوك البشري ،المتمثل في الأنشطة غير المشروعة يمكن السيطرة عليه إذا كانت هناك عقوبات صارمة حيث ان نظرية الردع كانت لها العديد من الافتراضات والمفاهيم في تفسير الظاهرة من خلال(**D'arcy & Herath, 2011, p. 650**) .

أ-يظل المورد البشري هو الحلقة الضعيفة، في استغلال النظام وسوء إدارته مما يأدي الى اختلال في الأمن الداخلي للمؤسسة.

ب-ترتبط معظم حوادث الكمبيوتر بالأعمال الداخلية، للمستخدمين المصرح لهم برغم من أحراز تقدم كبير في اكتشاف ومنع الهجمات، لا توجد حماية ضد مثل هذه الثغرات الأمنية.

ت-يأدي استغلال النظام المعلوماتي، على الرغم من الإجراءات الأمنية الفعالة والضرورية بسبب سوء السلوك البشري يعتبر، من التهديدات الداخلية للمؤسسة، سواء كانت ضارة أو عرضية أو غير قانونية.

3.4.2. نظرية حماية التحفيز

تري نظرية التحفيز ان المؤسسات تواجه العديد من المشكلات الأمنية بسبب عدم التزام الموظفين بسياسات الأمن الداخلي، وهذا راجع كونهم يفكرون في احتمال اتخاذ إجراءات (الكفاءة الذاتية) وما إذا كانت هذه الإجراءات ستؤدي إلى نتائج مرغوبة محددة (الاستجابة) (**Hsu & Shih, 2015, p. 12**).

أ-حيث تري، ان المؤسسة بحاجة إلى ضمان عدم تعرض أنظمة الكمبيوتر والبنية الرقمية ومعلوماتها للخطر.

ب-من خلال اتخاذ التدابير الأمنية المناسبة في مكانها.

ت-يستوجب التزام الموظفين بسياسة الأمنية داخل المؤسسة.

حيث أظهرت العديد من الدراسات ان الانتهاكات الأمنية نتيجة، عن تصرفات الخاطئة للعمال حيث يعد تجاهل الموظف للامتثال لسياسات الأمان، مشكلة رئيسية للمؤسسة وتشكل التهديدات الأمنية الناتجة عن هذا السلوك نصف جميع الخروقات التي تتعرض للها البنية الرقمية.

5.2.أهمية الأمن السيبراني

تعتبر السلامة والأمن محورًا مهمًا في حياة الإنسان، من خلال ووضع قواعد حديثة للأمن في ظل العولمة والتطور التكنولوجي، وإيجاد طرق لحماية الحياة وجعل الأمن أهم شاغل في الحياة مستخدمي الأنترانت، فهذه القواعد والوسائل تتطور مع تطور المجتمع وتجنب عواقب التنمية الاجتماعية.

أما من منظور التعقيد، لم يعد الأمن السيبراني مقصورًا على الحفاظ على الوجود البيانات الرقمية بل امتد، ليشمل العديد من المجالات الأمنية، تتعلق بالتطورات الاجتماعية والاقتصادية والسياسية على سبيل المثال (الأمن الفكري - الأمن الشخصي - الضمان الاجتماعي - الأمن المروري - الأمن البيئي - الأمن السياسي - الأمن الاقتصادي.. إلخ) أما فيما يخص الأمن السيبراني، يركز على الأمن في العالم افتراضي حيث يستخدم الأفراد الأجهزة الإلكترونية لتخزين المعلومات، وتعديلها ونقلها عبر الأنظمة المتصلة بالشبكة والهياكل المادية. (Goutam, 2015, p. 14)

فهو مكان غير مرئي تجري فيه الاتصالات والأنشطة المتعلقة بالإنترنت، فالفضاء السيبراني هو بيئة خيالية لا تكون فيها العناصر حقيقية ولا تمثل العالم الحقيقي وهي قاعدة مستخدمين تقارب 2.7 مليار شخص، توجد هذه المنصة بالكامل في العالم الرقمي مما يسهل تبادل المعلومات والمحادثات، حيث يخلق مساحة عالمية للأفراد لمشاركة آرائهم وأفكارهم وخدماتهم، مما يعزز الشعور بالمجتمع. تسمح مرونة المنصة لها بتجاوز الحدود الجغرافية والحكومية، ونموها لا يعوقه قيود مادية أو سياسية(Jackson, 2010, p. 25).

حيث للأمن السيبراني أهمية وهي على النحو التالي:

1. ممارسة تأمين المعلومات الإلكترونية جزءًا لا يتجزأ، من رفاهية الأفراد والعائلات والمؤسسات والحكومات والمؤسسات الأكاديمية، والشركات اليوم يجب على الآباء والأسر إعطاء الأولوية لحماية أطفالهم من الاحتيال عبر الإنترنت.

2.ضمان حماية البيانات المالية، من أجل الحفاظ على الاستقرار المالي للفرد. بالنسبة للمعلمين والطلاب والموظفين، يعد الإنترنت موردًا قيمًا قدم العديد من فرص التعلم ومع ذلك، فإنه يشكل أيضًا تهديدات محتملة يجب معالجتها لضمان سلامة جميع الأطراف المعنية.

3.يعتبر الأمن السيبراني من أهم الأساليب الوقائية لمواجهة الجريمة والذي انتهجته العديد من الدول مثل هولندا وكندا، للحفاظ على أمنها وتقليل معدل الجريمة.

4.كما تعد تنمية الوعي الأمني، أسلوباً وقائياً يجنب المجتمع ما يلحقه من تبعات اجتماعيه واقتصاديه ومعنوية للجريمة، يجب أن تعمل الدولة على تنميته وتطويره بما يخدم مصلحة الأمن والاستقرار.

5.ويؤدي عدم وجود الوعي الأمني، بشكل عام إلى ممارسة السلوكيات أو الأنشطة التي تقود الفرد لتهديد أمنه الشخصي وكذلك أمن المجتمع

3.الوعي السيبراني للجريمة الإلكترونية في الوسط الجامعي الجزائري

1.3.مفهوم الوعي السيبراني

في ظل تنامي الثورة التكنلوجية وتزيد استخدام تقنياتها في الجامعة وانتشار ثقافة التواصل الافتراضي، في المجتمع الجامعي حيث أصبح ملاحظ تزايد في نسب مستخدميها من طبة وأساتذة، وحتى الأدارة الجامعية وذلك يعود للجو انها الأجابية في العملية التعليمية والخدمات الرقمية حيث تسهل عملية استهلاك ومشاركة المحتوي علمي، في ذات الوقت تستخدم في أغراض، غير مشروعة حيث بات البعض يستخدمها في ارتكاب الجرائم الإلكترونية التي تعود بضرر، على الجامعة لاسيما في ظل نقص الوعي السيبراني لدي مستخدمي البيئة الافتراضية.

فالوعي السيبراني في مفهومه العام، هو القدرة على فهم الحاجة الى الأمن السيبراني والتعبير عنه بالدقة والوضوح والقدرة على الوصول الأمن لمعلومة من خلال أدراك الفرد لذاته وما يحيط به في البيئة الافتراضية إدراكا مباشرا، فهو أساس كل معرفة وهذا يعني فهم الأنسان لذاته ولي غيره في عملية التفاعل الافتراضي، معهم لتحقيق حاجياته ومصاحه وهو مدرك لذاته ولى غيره وللبيئة من خلال المواقف المختلفة التي تصادفه في عملية التفاعل الافتراضي (**Abawajy, 2014, p. 237**).

كمأنا، الوعي بأمن المعلومات يمكن تعريفه كمستوى الفهم الذي يمتلكه المستخدمون حول أهمية أفضل ممارسات أمن المعلومات عمومًا، يتمتع موظفو المؤسسات بمستويات متفاوتة من الوعي بالأمان، كما أنهم يشاركون بزيادة في أنشطة عبر الإنترنت خطيرة مثل الشبكات الاجتماعية والمدونات والرسائل الفورية، ويعد عدد كبير منهم غير مدركين لمخاطر الأمان التي يتعرضون لها أثناء القيام بذلك(**Shaw et al., 2009, p. 94**)

وبهذا، فالوعي السيبراني لا يتوقف على معرفة المهارات الأساسية للاستخدام تقنيات الحاسب والشبكات في تحديد مكان المعلومة وكيفية الوصول الأمن للها وتقيمها واستعمالها بشكال فعال بالجوانب الأمنية والوقائية والأخلاقية، حيث أن زيادة وعي السيبراني للمستخدمين داخل هذا الفضاء الرقمي من شأنه التقليل، من الاختراقات والاعتداءات التي تمس بأمن الجامعة وخصوصية المستخدمين من الوسط الجامعي.

فالوعي السيبراني هي قدرة المستخدمين للشبكة الأنترانت والوسائط التكنلوجية من طلبة وأساتذة وأعضاء الأدارة، هي قدرة على حماية معلوماتهم الشخصية وبياناتهم الرقمية خلال التفاعل الرقمي من خلال التميز بين المعلومات الحقيقة والمصادر الموثوقة، التي تكون في شكل مواقع او أشخاص فكثير ميتم مصادفة العديد من الأشخاص الانتهازين والمعلومات المضللة التي تهدد وتضر، بالنظام المؤسسة الجامعية ومستخدم ومن بينها الهجمات السيبرانية في عديد من صورها مثل الانتحال والسرقة والابتزاز والتهكير.....الخ(الرشيدي & المهداوي, **2023**ص**52**).

وذلك وفق لمعرفتهم بالأمن السيبراني وأساسيات التي ركز عليها بحكم ان هنالك علاقة بين معرفتهم وادراكهم، لما يحيط بهم في العالم الافتراضي والوعي بالاستخدام السليم للأجهزة والمواقع وحماية أنفسهم من الهجمات السيبرانية، التي تهدد حياتهم الافتراضية ومعلوماتهم الشخصية فكلما توفرت لدي الشخص المستخدم المعرفة ومقومات، والخبرات تجاها هذا المجال يكون له القدرة على تمية وعيه السيبيري، الذي يحقق له الأمن من خلال بناء قدراته تجاه إدارة المخاطر السيبرانية.

2.3. مفهوم الوعي بالجريمة الإلكترونية

أصبحت الإنترنت نظامًا اجتماعيًا فنيًا مكونًا من كافة نظم وجوانب الحياة البشرية التي تعتمد إلى حد ما على البرمجيات، ومع الدور المتزايد لهذا النظام، زادت أيضًا عدد الجرائم التي ترتكب باستخدام تقنيات الحواسيب، على الرغم من اقتراح العديد من النماذج لتحقيق في جرائم الإنترنت، إلا أن جريمة في الفضاء السيبراني عمومًا لا تُعتبر جريمة قابلة للعقاب.(**Ismailova & Muhametjanova, 2016, p. 33**)

فالوعي بالجريمة الإلكترونية هي أدارك الفرد للأعمال الغير المشروعة التي يتم استخدام الكمبيوتر فيها كأداة، هدف، أو كليهما، يمكن استخدام الكمبيوتر كأداة في العديد من الأنشطة الإلكترونية الغير قانونية، مثل التعاملات الوهمية والتلاعب والتغيير في بيانات الكمبيوتر. (**Paul & Aithal, 2018, p. 60**)

ومنه فالوعي بالجريمة الإلكترونية يجب أن يركز على أصناف الجريمة الإلكترونية قانونيا، فهنالك عدة أصناف تميزها عن الجرائم الأخرى فهي تختلف عن الجرائم التقليدية وهذا راجع لطبيعة المعلومات الخاصة كونها بيانات رقمية، وبناءً على حقيقة أن الأوصاف التي تعطي قيمة للأشياء المادية فقط، نص قانون العقوبات الجزائري على ثلاث أنواع من الجرائم المعلوماتية.

فوفقًا للمادة 394 مكررًا، يمكن تصنيف جريمة الدخول غير المشروع أو التواجد في أنظمة معالجة البيانات الآلية إلى إجراءين مختلفين، يتضمن الإجراء الأول الوصول إلى المعلومات والبيانات المخزنة، داخل نظام الكمبيوتر دون موافقة صريحة من الفرد المسؤول عن هذا النظام، الإجراء الثاني يتعلق بالبقاء داخل النظام دون إذن مناسب (بغدادي، **2019**، صفحة **186**)

كما تتناول المادة 394 مكرر 02 جريمة الانخراط في معاملات البيانات غير المشروعة يجرم الحكم الأولي، لهذه المادة مجموعة من الأفعال المحفوفة بالمخاطر التي إن لم تكن محظورة من شأنها أن تؤدي إلى ارتكاب جرائم إضافية، تتضمن العملية التي تؤدي إلى تنفيذ الجاني للجريمة عدة مراحل، تشمل هذه المراحل التصميم والبحث وجمع البيانات وكل ذلك بقصد تسهيل وصول الآخرين إليها، ثم يفترض الجاني السيطرة على البيانات إما عن طريق نشرها أو إتاحتها، أو الانخراط في تجارة تنطوي عليها. (بوهرين، **2021**، صفحة **55**)

ومن خلال هذا فالجريمة المعلوماتية لا تحدث على الكمبيوتر، بل تحدث ضد أحد مكونات نظام المعلومات، قد يحدث أيضًا من خلال استغلال هذا النظام غالبًا ما يكون هدف الجاني، هو الرغبة في إدخال تعديل على عناصر الإقرار المالي خلال مراحل العملية بما في ذلك الدخول أو المعالجة والخروج.

3.3. إدارة الأمن السيبراني والتوعية السيبرانية في الوسط الجامعي

تشكل الهجمات الإلكترونية تهديد على الجامعة بحكم أنها تشمل عديد من الأنشطة غير القانونية، التي يرتكبونها المتسللون والمحتلون عبر الأنترانت بغيت الوصول غير القانوني الى البيانات والمعلومات، خاصة بالمؤسسة الجامعية وأفرادها من خلال الاعتماد على الرسائل غير المرغوب بها والبرامج الخبيثة لتحقيق أهدافهم غير المشروعة.

حيث تضم الهجمات السيبرانية حسب دراسة Mahzan & Shahimi (2018) ثلاثة أنواع من المخاطر تتعلق بالسرية، وتكون في حالة تسريب المعلومات للمؤسسة او أفراد و اختراق البيانات، إضافة الى مخاطر الاحتيال و تعطل عن ممارسة الأعمال مما يأدي الى خلال في الأداء.(**Shahimi & Mahzan, 2018, p. 1257**)

ومن خلال هذا فقد أصبح أمن مؤسسة الجامعية من قضايا الأمن السيبراني لتحقيق الحماية نظام وشبكة وبرامج وبيانات المؤسسة، من مخاطر والهجمات السيبرانية للآن أدارة الأمن السيبراني في الجامعة الجزائرية يستوجب ان يكون في المقام الأول، لحماية الأشخاص والهياكل الاجتماعية وعمليات العمل والتقنيات، والمشاريع الرقمية التي أنشأتها وزارة التعليم العالي والبحث العلمي في إطار جهود رقمنة مؤسساتها التعلمية وتحسين الكفاءة والأداء لها.

ان أدارة الأمن السيبراني في مفهومها العام، هي عملية حد ومواجهة المخاطر السيبرانية للمؤسسة الجامعية حيث يدخل في إطار إدارة المخاطر في الوسط الجامعي والتي تهدد مورده البشري، وقد تأدي الى خروقات أمنية وخسائر مالية ومادية وهي نوع من المراجعة الداخلية ونشاط مستقل يقدم تأكيدات وتحسين عمليات الحوكمة و أدارة المخاطر والرقابة داخل الجامعة. (**Yang et al., 2020, p. 170**)

من خلال إدارة الأمن السيبراني، يمكن للمؤسسات التعليمية وضع خطط استراتيجية منظمة لحماية بنيتها التحتية والرقمية. يتضمن ذلك رصد أي عمليات غير مصرح بها تتعرض لها المؤسسة، ويعتبر هذا الدور مكملًا للعملية التعليمية والتكوين الأكاديمي. تتطلب هذه الخطط وضع إطار أمني يتماشى مع مؤشرات الأمان السيبراني العالمية، ويتضمن التركيز على التقييم الدوري للأمن في الجامعة.

من خلال هذا التقييم، يتم الكشف عن النقائص والثغرات التي يتوجب التركيز عليها سواء من الناحية التقنية أو الناحية البشرية، مثل زيادة الوعي لدى الأفراد في استخدام التكنولوجيا والوسائط المتعددة بشكل صحيح. من خلال تحقيق هذا الهدف، يمكن تجنب الأخطاء البشرية والتقنية داخل المؤسسة الجامعية وضمان سلامة البيانات والأنظمة. (أبو الخير& طه، **2023**، ص**14**)ومن خلال هذا يمكن تقديم تعريف أجرائي من الباحث حول الإدارة الأمن السيبراني على أنها جزء من الهيكل التنظيمي للمؤسسة التعلمية، ومكملة لدورها وأهدفها من خلال توفير الأمن للمورد البشري والمؤسسة الجامعية وخاصة في مراحلة التحول التعليم العالي الى تعليم المفتوح الذي يركز على التفاعل الافتراضي، من خلال الوسائط المتصلة بالأنترانت وتعمل هذه الأدارة على حماية البيانات الرقمية للمؤسسة والفرد، من خلال الحد من

الهجمات السيبرانية التي تهددهم او وضعة خطة استراتيجية أمنية تحدد فيها أهم الهجمات السيبرانية التي تهددهم فتعمل على الوقاية منها وتوعية بها.

4.3.أهداف تقيم الوعي السيبراني في الوسط الجامعي

تسعي أي جامعة، من خلال الأطار الأمني محدد لتحقيق بيئة مستقرة وتوفير شروط لتكيف داخل المؤسسة والتنظيم الأمثل لها وهذا راجع لمهام الرئيسية المتمثلة في انتاج ونشر البحوث المعرفة العلمية على الصعيد العالمي، وهي عرضة لمشاكل متنوعة فيما يخص الأمن السيبراني مثل السرقة الملكية الفكرية وسرقة خصوصيات الطلاب والموظفين بإضافة الى أخترق البوابات الرقمية المعتمدة، من طرفها وهذه من بين المشاكل التي توجهها كل جامعات الجزائرية والعالمية ومن بين الأهداف الرئيسة في عمل الأدارة الأمن السيبراني هي:

1.4.3. التعليم: وهذا من خلال أنشاء بيئة تعلمية للطلبة والأساتذة وتنظيم ملتقيات ومحاضرات تتناول مواضيع السلامة والأمن عند استخدام الأنترانت، حول أساسيات الأمن السيبراني وحفاظ علي بيانات وتواصل خلال استخدام مواقع التواصل الاجتماعي. **(Chou & Peng, 2011, p. 47)**

2.4.3. تحديد التهديدات الإلكترونية: ان في أطار الذي تعمل عليه إدارة الأمن السيبراني هو تحديد التهديدات الإلكترونية التي يمكن أن توجهها الجامعة وهي من التحديات التي أصبحت تشهدها خاصة، أن عملية تسجيل الطلبة والتوظيف أصبح ترتكز على التسجيل عن بعد عن طريق البوابات الرقمية التي، يمكن أن تشهد عمليات للانتحال الشخصية والتزوير كما يحتمل أن يقوم مجرمي الأنترانت بأنشاء موقع ويب مزيف للجامعة والاحتيال على الطلبة والأساتذة، ومن تحديد التهديدات المحتملة يمكن تسير كل ظروف والمشاكل التي قد تعرقل عملها قبل أن تحدث وهذا يدخل في جانب التبوء بالمخاطر.(السعبري & الزرقي**2019**, **473** ص)

3.4.3. بناء برنامج الأمني: من خلال برنامج الأمن السيبراني الذي تبنيه الأدارة على المدي القريب والبعيد لتقليل من ضعف نظامها، وشبكاتها التي تعمل في الفضاء الالكترونية والذي يتمشى مع قدراتها المادية والتقنية والبشرية، في مواجهة التهديدات الإلكترونية حيث يعتبر الأطار المرجعي الذي تتقيد به المؤسسة الجامعية، في فهم التحديات الجديدة في الجرائم السيبرانية والحلول الفعالة ذات كفاءة في تحقيق الأمن الشامل والتكيف والتوازن داخل المؤسسة.

ومن خلال هذا يمكن أن نعتبر للأدرة الأمن السيبراني للمؤسسة الجامعية أهداف تساير التحول الرقمي الذي تشهده الجامعات، من خلال التركيز على استراتيجية ذات معاير دولية من خلال تحديد التهديدات التي تستهدفها وتأثر على عملية التعلمية وأخلال في التوازن دخلها بناء على العديد من التقرير العالمية، التي تخص الجريمة الإلكترونية ودارسات الميدانية للباحثين في نفس مجال يسهل لها تصنيف التهديدات السيبرانية كما يسهل لها بناء برنامج يخص بيئتها الإلكترونية لتعامل، مع الأوضاع الحساسة والحرجة التي تهدد طلبتها وموظفيها و عملية التبادل ونشر العلمي بينها وبن المؤسسات على نطاق العالمي.

5.3.المؤسسات التنشئة الاجتماعية ودورها في تنمية الوعي السيبراني

في أطار تنمية الوعي السيبراني هنالك العديد من المؤسسات المختلفة مكلفة بتنشئة المجتمع وأفرادها وتطوير مهاراته، للآن حماية المجتمع من الجرائم المختلفة ليست مسئولية الجهات الأمنية وحدها بل يشاركها في، هذا كافة أفراد المجتمع الواحد للآن الخطر واحد والجهات المعنية بحماية والحفاظ، على تماسكه ويتحقق هذا بالتعاون في نشر الوعي السيبراني والذي يساهم بشكل كبير في حماية مستخدمي الأنترانت من الجرائم الإلكترونية. (زيدان وأخرون، **2018**، صفحة **267**)

ومن خلال هذا سوف نحدد العديد من المؤسسات التنشئة الاجتماعية المكلفة بتنمية الوعي السيبراني في المجتمع حيث انها تؤثر في سلوك العام للمجتمع وأفكارهم من خلال الأساليب تربوية وتهيئة نفسياً إلى جانب تنمية القدرات الكافية في استخدام تكنولوجيا الحديثة، وتتمثل المؤسسات التربوية وهي على النحو التالي:

1.5.3. الأسرة:

تعتبر أول مؤسسة تنشئة اجتماعية يترعرع فيها الطفل، حيث كانت في الماضي تعرفه بأساسية الأمن مثل تعريفه بالمواد الضارة والسلوكيات، السيئة وتأديبه عليها ومنعه من مخالطة الرفاق السيئين أما مع تطور التكنولوجي، أصبح يفرض عليها الواقع على رقابة الطفل في الواقع المادي والافتراضي من خلال (حواوسة، **2018**، صفحة **137**) :

- تنمية أدراكه للأساسيات الاستخدام السليم والأمن للوسائط الإلكترونية.
- تعريف الطفل بأساسية الحماية من خلال أسلوب الوالدين الذي يجمع بين النصح والإرشاد.

- استخدام المطبوعات والصوار لغرس الوعي الأمني للفرد المراهق خاصة في بداية سنواته الأولى للآن طفل يتعلم من الملاحظة.

ومن خلال هذا نستنتج أن للأسرة دور، هام وفعال في تنمية الوعي السيبراني للفرد في جميع مراحل حياته خاصة في مرحلة الطفولة، حيث يستمد الفرد من أسرته الوعي بالقيم الفكرية المستمدة من الثقافة الاجتماعية للمجتمع وتحدد له السلوك السليم.

2.5.3. المدرسة:

تعتبر المدرسة ثاني مؤسسة يتوجه للها الفرد بعد الأسرة حيث يتكون في الأطوار الثلاثة (ابتدائي، متوسط، ثانوي)، وهي مرحلة انتقالية في تنشئة الفرد من خلال تعمق أكثر في معرفة ما حوله حيث أن العولمة قد أثرت على مدرسة، من خلال تكوين المجتمع في أستخدم التقنيات الحديثة والوعي الأمن لتحقيق شعوره بالاستقرار وعدم تواجد خطر حوله من خلال (الطيار، **2017**، صفحة **167**) :

- أبراز له حقوقه ووجباته في جانب المواطنة الرقمية التي وصل لها المجتمع نتيجة ربطه بالأنترانت.
- تضمين البرامج التعليمة بالمواد التوعية بمخاطر الاستخدام غير الواعي والأدمان على الأنترانت.
- ربط المدرسة بالأسرة لتحقيق الدور التكاملي في تمية وعي الفرد في مجال الأمن السيبراني من ظاهرة الجريمة الإلكترونية التي تستهدفهم.

3.5.3. الوسائل الإعلامية:

أصبحت الوسائل الإعلامية من المؤسسات التنشئة الاجتماعية، راجع الى مدي تأثيرها على أراء وأفكار المجتمع في جميع المجالات (السياسية، الاقتصادية، الاجتماعية، الثقافية ...الخ) وبهذا فهيا نافذة للكل الأخبار العالمية، من خلال نقل السلوكيات السليمة للفرد من خلال نقل المعلومات عن طريق الأخصائيين في مجال الأمن السيبراني مما يأدي الى تنمية الوعي السيبراني للفرد ويكون هذا من خلال (بغدادي خ.، **2018**، صفحة **75**):

- التنسيق مع الأجهزة الأمنية والأعلام في نقل الإرشادات والتوصيات اللزمة في مواجهة الجريمة الإلكترونية.

- تنمية الوعي القانوني وثقافة التبليغ للمواطن حتى تكون له قدرة الكافية في اتخاذ السلوك اللزمة في حالة وقع ضحية للجريمة الإلكترونية.
- عرض المواضيع الحصص التلفزيونية حول مخاطر الجريمة الإلكترونية التي أصبح تحت حتمية وقوع ضحية لها او جناة خاصة إذا كإنو لا يدركون ما يفعلون.

4.5.3. الأجهزة الأمنية:

تعتبر الأجهزة الأمنية الموكل لها تصدي للهجمات والجرائم الإلكترونية او التقليدية من خلال موردها البشري الكفء، من حيث التكوين لهذا النوع من الظواهر التي تخل بأمن والاستقرار العام لدولة نتيجة التطور التكنولوجي السريع، ادي تحديث الإجراءات الوقائية التي لها دور في تنمية الوعي الرقمي والاستخدام الأمن للأنترانت من خلال (الجحني علي، 2002، صفحة 32):

- مشركة الأجهزة الأمنية في الملتقيات الوطنية والدولية والجامعات واللقاءات التليفزيونية للتوعية السيبرانية لكل أفراد المجتمع للاستفادة من خبراتهم في المجال الأمني.
- تأطير وتكوين الأفراد بشراكة مع المؤسسة الوطنية في مجال الحماية السيبرانية وتعريف بتقنيات الحماية.
- تفعيل الدور الكامل بين المدرسة والأسرة والأعلام لتحقيق لأهداف الأجهزة الأمنية في نشر الأمن وتنمية الوعي لتصدي لظاهرة الجريمة الحديثة.
- تفعيل دور التعاون بين الأجهزة الأمنية والأفراد مجتمع من خلال التبليغ والتصدي للسلوكيات المخلفة للقانون والقيم المجتمع.

ومن خلال هذا نستنتج أن تنمية الوعي السيبراني، تستوجب عملية تكاملية تكون بداية من الأسرة، باعتبارها اول مؤسسة يترعرع فيها الطفل فهيا والتي تغرس فيه أساسيات أدراك للمخاطر التي تواجهه، كمأن المدرسة، هي التي تساير وظيفة الأسرة من خلال المناهج التعلمية، اما الأعلام والأجهزة الأمنية تجمع بين العمل الميداني وجانب المعرفي والتوعوي لتحيق تنمية للوعي السيبراني الشامل.

ملخص الفصل

ونستنتج من خلال فصل الوعي السيبراني في الوسط الجامعي، كونه مفهوم حديث كان نتيجة التطور التكنلوجي ونقل السريعة في بنية الجامعة والوسائل المعتمدة في التعليم العالي والتوصل الاجتماعي، حيث كان الهدف الأساسي هو أبرا علاقة الوعي السيبراني بالوسط الجامعي من خلال تبين

أهم التحولات التي عرفتها الجامعة كمؤسسة، مثل تغير في طريقة التعليم وأدواته و تحولها من الواقع المادي الي افتراضي، وتعريف مجال الأمن السيبراني و أهدافه، وأهميته وذكر أهم نظريته المفسرة للأسباب التي تأدي الى ضعفة في حماية الرقمية والاختراق الإلكتروني وفي الأخير، تم تعريف كل من الوعي السيبراني والوعي بالجريمة الإلكترونية ومفهوم إدارة الأمن والتوعية السيبرانية، في الوسط الجامعي وأهداف تقيم الوعي السيبراني المؤسسات التنشئة الاجتماعية ودورها في تنمية الوعي السيبراني.

الفصل الرابع:

الإطار المنهجي والميداني للدراسة

IV. الفصل الرابع: الإطار المنهجي والميداني للدراسة

1 الإجراءات المنهجية للدراسة

1.1 منهج الدراسة

2.1 مجالات الدراسة

3.1 مجتمع الدراسة وعينته

4.1 أدوات جمع البيانات

5.1 إجراءات الدراسة

6.1 الأساليب الإحصائية

2 عرض وتحليل ومناقشة الجداول

1.2 عرض وتحليل الجداول المتعلقة بالبيانات الديمغرافية

2.2 عرض وتحليل الجداول المتعلقة بالسؤال الأول

3.2 عرض وتحليل الجداول المتعلقة بالسؤال الثاني

4.2 عرض وتحليل الجداول المتعلقة بالسؤال الثالث

5.2 عرض وتحليل الجداول المتعلقة بالسؤال الرابع

6.2 عرض وتحليل الجداول المتعلقة بالسؤال الخامس

7.2 عرض وتحليل الجداول المتعلقة بالسؤال السادس

8.2 تحليل ومناقشة النتائج الجزئية

9.2 الاستنتاج العام للدراسة

1 الإجراءات المنهجية للدراسة

1.1 منهج الدراسة

تفرض البحوث العلمية على الباحث إتباع أساليب، ومناهج علمية محددة حسب تخصصه ونوع دراسته لتحقيق النتائج وأهداف الرئيسة للبحثة، أي باحث من خلال الدراسة الميدانية لبحث تخرجه، وهدفه الرئيسي هو الوصول إلى المعرفة العلمية اليقينية والتي لا يمكن تحقيقها إلا بواسطة استخدام المنهج العلمي، الذي يوجهه إلى طريقة تعامله مع القاعدة المعرفية والمعلوماتية المتاحة لتحقيق أهداف الدراسة، وقد عرف مفهوم المنهج عديد من التعريفات وهي على النحو التالي:

حسب " **موريس انجرس** " بأنه هو مجموعة الإجراءات والخطوات الدقيقة المتبناة من أجل الوصول إلى نتيجة، كما يمثل المسألة الهوية، فالإجراءات المستخدمة أثناء اعداد البحث وتنفيذه هي التي تحدد النتائج وعليه يجب اتباع تلك السلسلة من المراحل المتتالية ينبغي استخدامها، بكيفية منسقة ومنظمة (موريس، 2004، ص36).

حسب " **منطق بروويال** " فن التنظيم الصحيح لسلسلة من الأفكار العديدة من أجل الحقيقة والبرهنة عليها (جندلي، ص 13).

اما المنهج عند "**رونز**" هو اجراء يستخدم في بلوغ غاية محددة (القاسم، 2003، ص 52).

وتماشيا مع طبيعة موضوع البحث الذي يجريه الباحث حول **مستوي الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الالكترونية**، ولتحقيق أهداف الدراسة اعتمد الباحث المنهج الوصفي الارتباطي، للوصول إلى نتائج الدراسة بعد جمع المعلومات ولكونه المنهج المناسب لهذه الدراسة، فضالاً عن استخدام الاستبانة كوسيلةً لجمع البيانات وقد تم توظيف هذا المنهج في دراستنا بهدف إلى وصف الظاهرة محل الدراسة، كيفيا و كميا بين بحثا عن العلاقة بين الوعي السيبراني و الوعي بالجريمة الإلكترونية ،لدي فئة طلبة كلية العلوم الإنسانية و الاجتماعية لجامعة جيلالي بونعامة بخميس مليانة

بالجزائر، من خلال تشخيصها وإلقاء الضوء على جوانبها المختلفة، وجمع المعلومات اللازمة عنها وفهمها وتحليلها من اجل الوصول إلى نتائج موضوعية في ضوء فرضيات الدراسة.

2.1 مجالات الدراسة

يتوقف تعميم النتائج التي ستتوصل اليها دراستنا، الراهنة على عدة عوامل ومحددات هي كالتالي:

1.2.4. المجال البشري: طبقة هذه الدراسة على طلبة وطالبات كلية العلوم الإجتماعية والإنسانية بجامعة جيلالي بونعامة بمدينة خميس مليانة، ولاية عين الدفلى خلال السنة الدراسية 2023/2022 موزعين على قسمين :قسم العلوم الإنسانية، وقسم العلوم الاجتماعية.

2.2.4. المجال المكاني: أجريت هذه الدراسة في جامعة جيلالي بونعامة بمدينة خميس مليانة بولاية عين الدفلى التي تبعد عن الجزائر العاصمة 140 كيلومترًا غربا، كانت في سنة 1991 المدرسة الوطنية للمناجم وهي الأول على مستوي الولائي، وفي 1995 تم تحويلها المعهد الفني للزراعة، كفرع لجامعة سعد دحلب البليدة ويدخل هذا في أطار توسيع تخصصات العلمية وفتح قطاعات علمية جديدة، وفي 18 من شهر سبتمبر سنة 2001 نتيجة للعمل المتوصل وجهود مبذولة من طرف الفاعلين في معهد تم ترقيته الى مركز جامعي مستقل.

وفيما بعد، تم تحويل هذا المركز إلى جامعة تضم حاليًا ست كليات ومعهدًا واحدًا ويبلغ عدد الطلبة المسجلين في كلية العلوم الإنسانية والاجتماعية (4548) طالبة وطالبات موزعة على قسمين، حيث بلغ عدد طلبة المسجلين في قسم العلوم الإنسانية (2412) اما بنسبة لقسم العلوم الاجتماعية فقد بلغ عدد طلبته المسجلين فيه (2136) طالبة وطالبات.

3.2.4. المجال الزماني: لقد مرت دراستنا بثلاث مراحل أساسية بعد التسجيل الأول للطور الدكتوراه خلال سنة الدراسية 2021/2020 تم تحديد عنوان الدراسة الموسوم ب **"مستوي الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الالكترونية"** حيث تم من خلاله تم تحديد سؤال

الانطلاق، خاص بموضوع البحث وتوجه نحو مرحلة الاستكشافية للموضوع من خلال قرأه الدارسات السابقة التي درست متغيرات الموضوع، ومنها تم ضبط الخطة النظرية للأطروحة.

اما في سنة الدراسة 2022/2021 التي كان فيها انتاج علمي متمثل في مقال الأول متعلق بالموضوع إضافة الى كتابة الأطار النظري للأطروحة، وأجراء دراسة استطلاعية مع فئة المتخصص في الموضوع لتحديد زاوية البحث النهائية، اما في سنة الدراسة 2023/2022 تم فيها ضبط النهائي للأسئلة الدراسة وتحديد الأداة النهائية بعد توجيهها لتحكيم، تم توزيع الاستبانة على طلبة كلية العلوم الاجتماعية والإنسانية بعد حصول على موفقة من عميد كلية.

3.1 مجتمع الدراسة وعينته

تكون مجتمع الدراسة من طلبة وطالبات كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة بمدينة خميس مليانة بولاية عين الدفلى في السداسي الثاني من السنة الدراسية 2023/2022 والبالغ عددهم (4548) طالبة وطالبات حسب تقرير عميد كلية ملاحق رقم (1) للعام الدراسي 2023/2022 ونظرًا لتباين واختلاف السمات في مجتمع الدراسة، يعتمد تحديد حجم عينة الدراسة على نسبة الخطأ ودرجة الثقة المرغوبة في النتائج، وفي هذا السياق نسعى للوصول إلى درجة ثقة تبلغ 95% بمستوى دلالة يقدر بـ 0.05.

نتيجة لتصنيف طلبة كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة بمدينة خميس مليانة بولاية عين الدفلى الى قسمين: علوم انسانية، علوم اجتماعية، والى مستويين لسانس، ماستر هذا التصنيف يفرض علينا اختيار عينة الدراسة وفقًا لشروط معينة، بهدف تمثيل جميع فئات المجتمع الأصلي وتقليل الانحراف اعتمدنا على معادلة **ريتشارد جيجر** في تحديد حجم العينة:

$$n = \frac{\left(\frac{z}{d}\right)^2 X(P)^2}{1 + \frac{1}{N} \quad \left[\left(\frac{z}{d}\right)^2 X(P)^2 - 1\right]}$$

وتكونت عينة الدراسة من 355 طالب وطالبة وتم اختيارها بطريقة المعاينة العشوائية الطبقية لوجود قسمين في الكلية قسم علوم انسانية، وقسم علوم اجتماعية، وكل قسم مقسم الى مستويين لسانس، ماستر من مجتمع الدراسة والجدول (1) و (2) يوضح ذالك.

جدول (1): توزيع أفراد مجتمع البحث لكلية العلوم الإنسانية والاجتماعية للجامعة جيلالي بونعامة تبعا لمتغير نوع القسم والمستوي الدراسي.

كلية العلوم الإنسانية والاجتماعية	لسانس	ماستر	المجموع
قسم علوم إنسانية	1381	1031	2412
قسم علوم اجتماعية	1470	666	2136
المجموع	2851	1697	4548

جدول (2): توزيع أفراد عينة الدراسة تبعا لمتغير المستوي الدراسي ونوع القسم.

كلية العلوم الإنسانية والاجتماعية	لسانس	ماستر	المجموع
قسم علوم إنسانية	112	70	182
قسم علوم اجتماعية	131	42	173
المجموع	243	112	355

ولسحب مفردات الدراسة تم تقسيم كلية الي طبقتين، حسب مستوي الدراسي للسانس وماستر للكل قسم من أقسام الكلية، ولجأنا الى السحب المنتظم لضمان أكبر درجة تمثيلية لعينة الدراسة، حيث تم اعطاء مفردات العينة المسحوبة من كل طبقة أرقاما متسلسلة بد تسجيل أسماء الطلبة وتم تحديد مسافة الانتظام، خاصة بالسحب 13 وكان رقم بداية السحب هو،1 ويوضح الجدول الثاني حجم أفراد العينة من كل قسم وحسب المستوي الدراسي للطلبة كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة بمدينة خميس مليانة بولاية عين الدفلى.

4.1 أدوات جمع البيانات

تعتبر مرحلة البيانات مرحلة جد حساسة في البحث ، فهي تحتاج إلى عناية كبيرة من طرف الباحث لان الاختيار الصائب و الأمثل للأداة التي ستعتمد في جمع البيانات سيساعد في تسهيل جمعها بأكبر دقة ممكنة ، و الأكيد أن اختيار أدوات جمع المعلومات لا يكون بمعزل عن طبيعة الدراسة و نوعيتها و الأهداف المرجوة من تلك المعلومات ، و كذا الظروف البحثية التي ستجرى فيها الدراسة التطبيقية ، و بالتالي فان اختيار الأداة يكون بشكل منهجي و يقوم الباحث بتصميم الأداة وفقا لأهداف البحث و خصائص القاعدة المعرفية التي يستقي منها البيانات.

قام الباحث بإعداد استبانة تتألف من 50 فقرة لقياس مستوي الوعي السيبراني لطلبة وطالبات كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة وعلاقته بمستوي وعيهم بالجريمة الإلكترونية وهذا بعد رجوع الى الدراسات السابقة ذات الصلة مثل **مينال شاوهان وأربنا (2012)**، أنوبريت كور موخا **(2017)**، غدير برنس وعبد الكريم عوده الله الخرابشة **(2020)**، نهي مصطفي كمال أبو كريشه **(2022)**، حمد بن حمود السواط **وآخرون (2020)** ايمان عبد الفتاح عبابنه **(2022)** عبد الله بن حجاب القحطاني **(2022)**.

وقد اشتملت الاستبانة على أربع محاور أساسية الأتية وهي:

- **المحور البيانات الشخصية:** قد تضمنت أسئلة متعلقة بالبيانات الشخصية لطلبة (الجنس، السن، المستوي التعليمي، نوع القسم) من اجل التعرف على السمات الشخصية للمبحوثين، وتكون هذا المحور من (4) أسئلة.
- **محور الاول:** قد تضمن (15) سؤال حول الوعي السيبراني، والجريمة الالكترونية من منظور الطلبة للاكتشاف، مدي المام الطلبة حول موضوع الجريمة الإلكترونية كظاهرة برزت نتيجة التطور التكنلوجي، ووعيهم السيبراني تجاه الاستخدام الأمن للأنترانت.

- **المحور الثاني:** قد ركز هذا المحور على تقيم أفراد العينة، حول درجة وعيهم السيبراني حيث تعد إجابات المبحوثين فهما للمجال الأمن، والوعي السيبراني وماهيته إضافة الاستخدام الأمن للأنترانت، وسبل تعرف على سبل تعزيز الوعي السيبراني من وجهة نظره.
- **المحور الثالث:** قد ركز هذا المحور على تقيم أفراد العينة حول درجة، وعيهم بالجريمة الإلكترونية كظاهرة منتشرة في الوقع الافتراضي، حيث من خلال هذا المحور سوف يتم تقيم درجة وعيه لها من جانب المعرفي، والقانوني ومدي ادراكه لخطورتها.

ولحساب كل من درجة وعي السيبراني، والوعي بالجريمة الإلكترونية للطلبة وطالبات كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة، من خلال المحورين الثاني والثالث تم الاعتماد على مقياس خماسي، الذي تراوح بين (5-1) فتمثل القيمة (5) اعلى قيمة والتي تشير الى عالي جدا، وتمثل قيمة (1) أدني قيمة والتي تشير الى منخفض جدا، وتم حساب درجة تقدير الوعي السيبراني، والوعي بالجريمة الإلكترونية لطلبة وطالبات كلية العلوم الاجتماعية والإنسانية للجامعة جيلالي بونعامة وفق المعادلة الأتية، والجدول(3) يوضح تقدير الدرجة.

$$\frac{\text{أكبر قيمة} - \text{أصغر اقيمة}}{\text{عدد فئات}} = \frac{(5-1)}{3} = 1.33$$

جدول (3): تقديرات المستوي لقيمة المتوسطات الحسابية

قيمة المتوسط	تقدير المستوي
1.00 - 2.33	منخفض
2.34 – 3.67	متوسط
3.68 – 5.00	مرتفع

1.4.4. صدق أداتي الدارسة:

صدق المحكمين هو المظهر العام للاختبار أو الصورة الشكلية للأداة، ويتعلق بعناصر مثل الأسئلة المستخدمة وطريقة صياغتها، فضلاً عن مدى وضوح العبارات، كما يشمل هذا النوع أيضًا قدرة الأداة على التأقلم مع السياق الذي صُمم من أجله.

حيث تم استخدام الصدق الظاهري للتحقق من صحة أداة الدراسة، من خلال عرضهما على مجموعة من المحكمين ذوي الاختصاص والخبرة في مجال علم اجتماع الجريمة والانحراف وعددهم 5 محكمين كما هو موضح في **الملحق 3**.

تم استخدام هذه الأداة لتحديد مدى انتماء الفقرات لموضوع الدراسة وصلاحيتها، ولتحديد ما إذا كانت بحاجة إلى التعديل، تم اختيار الفقرات التي حصلت على موافقة بنسبة 80% أو أكثر من المحكمين، وتم تعديل الفقرات التي وافق عليها 60-70% من المحكمين، تم حذف الفقرات التي وافق عليها 50% فأقل بعد التحكيم، أصبح عدد فقرات الاستبانة النهائي 50 فقرة بالنسبة لمحور الوعي السيبراني كما هي، وعدد فقرات محور الوعي بالجريمة الالكترونية بقيت كما هو موضح في **الملحق 5.**

2.4.4. صدق البناء:

للاستخراج صدق للبناء لكل من مقياس المحور الثاني خاص بدرجة وعي السيبراني والمحور الثالث لمقياس وعي بالجريمة الإلكترونية، تم احتساب معامل الاتساق الداخلي من خلال حساب معامل ارتباط بيرسون بين درجة كل عبارة والدرجة الكلية للبعد الذي تنتمي إليه، هذا الإجراء يهدف إلى التحقق من صدق الأداة بشكل أوسع، تم توزيع الاستبيان على عينة استطلاعية من خارج عينة الدراسة مكونة من 40 فرد والجدول (4) يبين ذلك.

جدول (4): معاملات الارتباط بين الفقرات والدرجة الكلية للمحور الوعي السيبراني

المحور الثاني: الوعي السيبراني					
رقم *فقرة*	معامل الارتباط	رقم *فقرة*	معامل الارتباط	رقم *فقرة*	معامل الارتباط
01	,394**	07	,626**	13	,524**
02	,554**	08	,479**	14	,603**
03	,404**	09	,552**	15	,697**

04	,500**	10	,644**	16	,625**
05	,367**	11	,403**	17	,489**
06	,502**	12	,744**	18	////

* دالة إحصائيا عند مستوى الدلالة (0.05). ** دالة إحصائيا عند مستوى الدلالة (0.01)

جدول (5): معاملات الارتباط بين الفقرات والدرجة الكلية للمحور الوعي بالجريمة الإلكترونية

المحور الثالث: الوعي بالجريمة الإلكترونية					
رقم *فقرة*	معامل الارتباط	رقم *فقرة*	معامل الارتباط	رقم *فقرة*	معامل الارتباط
01	,418**	07	,776**	13	,201**
02	,583**	08	,488**	14	,680**
03	,375**	09	,481**	15	,589**
04	,527**	10	,486**	16	,479**
05	,647**	11	,579**	17	,424**
06	,685**	12	,673**	18	,436**

* دالة إحصائيا عند مستوى الدلالة (0.05).

** دالة إحصائيا عند مستوى الدلالة (0.01).

وتجدر الإشارة أن معاملات الارتباط جميعها كانت ذات درجات مقبولة ودالة إحصائية، ولذلك لم يتم حذف أي من هذه الفقرات.

3.4.4. ثبات الأداة:

للتأكد من ثبات أداة الدراسة، فقد استخدمت طريقة الاختبار حساب معامل الثبات بطريقة الاتساق الداخلي حسب معادلة كرونباخ ألفا، حيث يستخدم هذا الاختبار لتقدير مقدار الثبات والموثوقية من خلال قياس الترابط الداخلي بين عبارات الاستبيان، وتتراوح قيمة معامل ألفا كرونباخ بين 0 و1، وكلما اقتربت القيمة من 1، كان ذلك دليلاً على استقرار الاستبيان وعموماً، يُعتبر معامل ألفا كرونباخ الذي يتجاوز 0.70 كحد أدنى مؤشراً جيداً ومقبولاً للثبات إذا ارتفع المعامل إلى 0.8، يُعتبر ذلك مؤشراً على وجود مستوى ممتاز من الثقة والاستقرار في الاستبيان.

جدول (6): معاملات الثبات للمحور الوعي السيبراني والوعي بالجريمة الإلكترونية

الرقم	المحور	كرونباخ ألفا
01	الوعي السيبراني	,737
02	الوعي بالجريمة الإلكترونية	,871

الجدول السابق يعكس نتائج استقرار أداة الدراسة باستخدام طريقة معامل ألفا كرونباخ يظهر أن درجات استقرار الاختبار كانت مقبولة عمومًا لجميع أبعاد ومحاور الاستبيان. في سياق المحور الثاني، الذي يتناول الوعي السيبراني لدي طلبة كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة، وصل معامل الثبات إلى 0.737 في المقابل، وعلى مستوى المحور الثاني، الذي يركز على الوعي السيبراني لدي طلبة كلية العلوم الإنسانية والاجتماعية بجامعة خميس مليانة، وصل معامل الثبات إلى 0.871 وبفضل هذه النتائج، يمكن توزيع الاستبيان في شكله النهائي على عينة الدراسة بعد التحقق من صدقه واستقراره، وهذا يمنحنا الثقة في فعالية الأداة للإجابة على أسئلة الدراسة واختبار فرضياتها وتحليل وتفسير نتائجها.

5.1 إجراءات الدراسة

بعد التحقق من صدق أداة الدراسة وثباتها، وتحديد مجتمع الدراسة وتعيينها من الأخصائيين الحصول على الموافقات الرسمية لتسهيل مهمة الباحث في تطبيق أدوات الدراسة لجمع البيانات المطلوبة. وتوضح الملحقات 2، وقد تم اتخاذ الخطوات التالية:

1- الحصول على كتاب تسهيل المهمة من عميد كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة بخميس مليانة. (الملحق 1).

2- الحصول على عدد الطلبة الكلي للمسجلين في كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة بخميس مليانة من طرف نائب عميد الكلية. (الملحق 5).

4- تطبيق الاستبيانات على عينة الدراسة.

5- جمع البيانات.

6- تحليل البيانات إحصائيًا والتوصل إلى النتائج.

7- تفسير النتائج ومناقشتها.

8- كتابة التقرير النهائي للرسالة الدكتوراه.

6.1 الأساليب الإحصائية

من أجل تحقيق أهداف الدراسة وتحليل البيانات التي تم جمعها من خلال استخدام الاستبيان، تم الاستعانة بمجموعة متنوعة من الأساليب الإحصائية الوصفية والاستدلالية المناسبة لمعالجة بيانات الدراسة باستخدام البرنامج الإحصائي SPSS (الحزمة الإحصائية للعلوم الاجتماعية) الإصدار 22، الأساليب الإحصائية المستخدمة في تحليل البيانات تشمل:

1. **معامل الارتباط بيرسون** (Coefficient Correlation Pearson) لقياس الترابط الداخلي والصدق البناء للاستبيان، وكذلك لقياس العلاقة بين متغيري الدراسة.
2. **معامل ألفا كرونباخ** (Coefficient Alpha s'Cronbach) لقياس الثبات في البيانات.
3. **النسب المئوية والتكرارات** (Percentages & Frequencies) لوصف البيانات الشخصية لعينة الدراسة.
4. **المتوسط الحسابي** (Mean) وذلك لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد الدراسة عن كل عبارة من عبارات أبعاد المحور الأساسية، مع العلم أنه يفيد في ترتيب العبارات حسب أعلى متوسط حسابي، ولتفسير مدى الاستخدام أو مدى الموافقة على العبارة يتم كما سبق أن وضحناه في المحك المعتمد في الدراسة.
5. **الانحراف المعياري** (Deviation Standard) للتعرف على مدى انحراف استجابات أفراد الدراسة لكل عبارة من عبارات لكل محور من محوريها الرئيسيين، عن متوسطها الحسابي ويوضح الانحراف المعياري التشتت في استجابات أفراد الدراسة لكل عبارة من عبارات أبعاد الدراسة إلى جانب محوريها الرئيسيين، فكلما اقتربت قيمته من 0 كلما تركزت الاستجابات وانخفض تشتتها بين المقياس (إذا كان الانحراف المعياري 1 صحيحا فأعلى فيعني عدم تركز الاستجابات وتشتتها).
6. **اختبار (T) للعينتين المستقلتين** (test-T Samples Independent) الاختبار الفروق بين متغيرات الدراسة واختبار فرضياتها، ويستخدم للمقارنة بين مجموعتين مستقلتين.

7. **اختبار تحليل التباين الأحادي** (test variance of analysis way-One) الاختبار الفروق بين متغيرات الدراسة واختبار فرضياتها، ويستخدم للمقارنة بين عدة متوسطات لمجموعات مستقلة.

2 عرض وتحليل ومناقشة الجداول

1.2 عرض وتحليل الجداول المتعلقة بالبيانات الديمغرافية

الجدول (7) يوضح توزيع أفراد عينة الدراسة حسب متغير الجنس

الجنس	التكرار	النسبة المئوية
ذكر	153	%43,1
أنثى	202	%56,9
المجموع	355	%100

نلاحظ من خلال الجدول، أن نسبة 56,9% من أفراد العينة من جنس الأناث في حين أن، نسبة 43,1% تمثل الذكور.

ونستنتج من خلال معطيات الجدول، أن كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة، تعرف اقبال من جنس الإناث على تخصصاتها مقابل جنس الذكور بحكم العديد من التخصصات التي تناسبهم في القطاع الوظيفي مثل علوم التربية، علم النفس، علوم الأعلام والاتصال ...الخ.

الجدول (8) يوضح توزيع أفراد عينة الدراسة حسب متغير السن

السن	التكرار	النسبة المئوية
من 17 سنة الى 21سنة	107	%30,1
من 22 سنة الى 26 سنة	158	%44,5
من 27 فما فوق	90	%25,4
المجموع	355	%100

نلاحظ من خلال الجدول، أن نسبة 44,5% من أفراد العينة تتراوح أعمارهم من 17 سنة الى 21سنة في حين أن، نسبة 30,1% تتراوح أعمارهم من 22 سنة الى 26 سنة اما بنسبة لفئة التي تتراوح أعمارهم من 27 فما فوق قد قدرت نسبتها ب25,4%.

ونستنتج من خلال معطيات الجدول، أن كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة، أن أكبر عدد من طلبة تتروح أعمارهم بين 17 و26 سنة وهذا نتيجة لعديد من الإصلاحات التربوية التي شهدتها الأطوار الثلاثة من التعليم الابتدائي، المتوسط، الثانوي وهذا مساهم في التحاق الطلبة بالجامعة في سن صغير أما بنسبة للفئة العمرية 27 فما فوق وهي من الفئات التي تتم دراستها لترقية ورفع المستوي العلمي.

الجدول (9) يوضح توزيع أفراد عينة الدراسة حسب متغير المستوي التعليمي

المستوي التعليمي	التكرارات	النسبة المئوية
لسانس	243	%68,5
ماستر	112	%31,5
المجموع	355	%100

نلاحظ من خلال الجدول، أن نسبة 68,5% من أفراد العينة من طلبة لسانس في حين أن، نسبة 31,5% تمثل طلبة الماستر.

ونستنتج من خلال معطيات الجدول، أن كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة، أكبر عدد من طلبتها مسجلين في طور لسانس مقابل طلبة ماستر الذي يشهد عزوف عن تسجيل في مرحلة الماستر، عكس سنوات الفائتة هذا نتيجة منحة البطالة التي قدمتها السلطات الدولة الجزائرية لحاملي الشهادات.

الجدول (10) يوضح توزيع أفراد عينة الدراسة حسب متغير القسم

القسم	التكرار	النسبة المئوية
العلوم الاجتماعية	173	%48,7
العلوم الإنسانية	182	%51,3
المجموع	355	%100

نلاحظ من خلال الجدول، أن نسبة 51,3% من أفراد العينة من قسم العلوم الإنسانية في حين أن، نسبة 48,7% من قسم العلوم الاجتماعية.

ونستنتج من خلال معطيات الجدول، أن كلية العلوم الاجتماعية والإنسانية لجامعة جيلالي بونعامة، أكبر عدد من طلبة مسجلين في قسم العلوم الإنسانية وهو أكثر جذب للجنس الإناث بحكم توفر تخصص الأعلام والاتصال وتخصص، التاريخ على عكس تخصصات قسم العلوم الاجتماعية التي تتوفر عليها تخصص الفلسفة وعلم الاجتماع.

2.2 عرض وتحليل الجداول المتعلقة بالسؤال الأول: ما هو الوعي السيبراني والجريمة الإلكترونية من وجهة نظر طلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة؟

جدول (11): يبين استخدام الطلبة للأنترانت:

استخدم الأنترانت	التكرار	النسبة المئوية
دائما	189	% 53.23
احيانا	100	% 28.17
نادرا	66	% 18.60
المجموع	355	%100

نلاحظ من خلال هذا الجدول، أن نسبة 53.23% من الطلبة يستخدمون الأنترانت دائما مقابل، 28.17% من نسبة الطلبة يستخدمون الأنترانت أحيانا، في حين أن، 18.60% تمثل نسبة الطلبة يستخدمون الأنترانت نادرا.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة تعرف استخدام عالي للأنترانت بتكرار قدره 189 طالب، ونسبة مئوية 53.23% من مجموع العام حيث، يتميز الطلاب الذين يستخدمون الإنترنت بمستوى عال من الاستخدام، والاعتماد على الأنترانت بشكل كبير في حياتهم اليومية، راجع لتنوع الاستخدامات الإنترنت مثل التواصل الاجتماعي حيث ان كل الطلبة في الجامعة الجزائرية يستخدمون فيس بوك، وانستغرام بإضافة الي البحث عن المعلومات والمصادر الأكاديمية وهذا راجع الي اعتماد وزارة التعليم العالي والبحث العلمي في السنوات الأخيرة على نظام التعليم عن بعد، والذي يفرض على الطالب استخدام

الأنترانت وعلاوة على هذا، فالترفيه وللعب الألعاب الإلكترونية، وغيرها من الأغراض يعد الإنترنت جزءًا أساسيًا من حياتهم ومن ثقافتهم الاجتماعية.

أما بنسبة لطلبة التي تعرف استخدام أحيانا للأنترانت بتكرار قدره 100 طالب، ونسبة مئوية 28.17 %من مجموع العام حيث، يستخدم الطلاب في هذا المستوى الإنترنت بشكل أقل من المستوى العالي من خلال التركيز عليها في بعض الأغراض مثل البحث العلمي والاتصال بالأصدقاء والزملاء، يمكن أن يكون استخدامهم للإنترنت مرتبطًا ببيئتهم الاجتماعية والثقافية، حيث أنهم قد يستخدمون الإنترنت بشكل محدود بسبب عدم وجود أساليب تواصل أخرى أو عدم توافر الإنترنت بشكل واسع في مجتمعاتهم.

أما بنسبة لطلبة التي تعرف استخدام نادرا للأنترانت بتكرار قدره 66 طالب، ونسبة مئوية 18.60%من مجموع العام حيث، يستخدم الطلاب في هذا المستوى الإنترنت بشكل قليل جدًا وغالبًا ما يكون الاستخدام مرتبطًا بأغراض محددة مثل البحث عن وظيفة أو الاتصال بأفراد العائلة والأصدقاء البعيدين.

جدول (12): يبين الساعات التي يقضيها الطلبة على للأنترانت:

الساعات التي تقضيها على للأنترانت	التكرار	النسبة المئوية
أقل من ساعة	75	%21.13
من ساعة الى 3ساعات	60	%16.90
أكثر من 3ساعات	220	%61.97
المجموع	355	%100

نلاحظ من خلال هذا الجدول أن نسبة 61.97% من الطلبة يستخدمون الأنترانت أكثر من 3ساعات، مقابل نسبة 21.13% الطلبة يستخدمون الأنترانت أقل من ساعة في حين أن 16.90% تمثل نسبة الطلبة يستخدمون الأنترانت من ساعة الى 3ساعات.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة تعرف استخدام أكثر من 3ساعات للأنترانت بتكرار قدره 220 طالب، ونسبة مئوية 61.97% من مجموع العام حيث نتيجة للحاجة إلى إنجاز الأعمال، الأكاديمية والأبحاث مقدمة من طرف الأساتذة إليهم في إطار تكوينهم في طورين لسانس وماستر، ويعتمد هذا الأمر على نوعية التخصص مثل تخصصات العلوم الإنسانية والاجتماعية والتي، تعرف توافر

مقالات العلمية والكتب ذات المصادر الإلكترونية اللازمة لإنجاز العمل البحثي، كما أصبحت عديد من الامتحانات التي يتم أنجازها عن بعد في الجامعة الجزائرية، والتي تفوق ثلاث ساعات للاختبار مستوي الطالب وتفرض عليه استخدام الأنترانت.

أما بنسبة لطلبة التي تعرف استخدام أقل من ساعة للأنترانت بتكرار قدره 75 طالب ونسبة مئوية 21.13%من مجموع العام، حيث هنالك العديد من العوامل التي لها تأثير على مدة الاستخدام للأنترانت مثل تفضيل الطالب المصادر المكتبية، على المصادر الالكترونية في عملية إنجازه للأبحاث الموكلة اليه من طرف الأساتذة وتفضيله التفاعل الاجتماعي الحقيقي في كسب المعلومة العلمية، مثل التوجه الى الأساتذة وتقديم اليه إرشادات فما يخص طريقة الإنجاز وخطوات التي يستوجب عليه اتباعها في ذالك، بإضافة الى قيود الوقت والجدول الزمني للطالب وهذا بنسبة لتخصصات العلوم الإنسانية والاجتماعية حيث ان برنامج تعليمي خاص بها كل مواده ترتكز على البحوث اكثر من الدروس النظرية، لهذا فطالب مفروض عليه تنظيم وقته بين التفاعل الافتراضي والحياة الشخصية والبحث العلمي.

أما بنسبة لطلبة التي تعرف استخدام من ساعة الى 3ساعات بتكرار قدره 60 طالب ونسبة مئوية 16.90%من مجموع العام، من بين العوامل التي تميز هذه الفئة تجمع بين التفاعل مع الأصدقاء وعائلتهم في مواقع التواصل الاجتماعي خاصة بنسبة للفئة الطلبة الداخلين في الإقامات الجامعية، إضافة الى الاستخدام المتعلق بالتعليم واعتماد على الأنترانت كوسيلة لتخفيف من الضغوطات الحياة واستمتاع، باللعب ومشاهدة الأفلام واستماع للموسيقي.

جدول (13): يبين أسباب استخدامك الطلبة للأنترانت:

أسباب استخدامك الطلبة للأنترانت	التكرار	النسبة المئوية
التعلم	126	%35.49
العمل	60	%16.90
الدردشة وتكوين صدقات	99	%27.90
مشاهدة الأفلام والبرامج	70	%19.71
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن نسبة 35.49% من الطلبة يستخدمون الأنترانت للتعلم مقابل نسبة 27.90%، من الطلبة يستخدمون الأنترانت للدردشة وتكوين صدقات في حين أن 19.71% تمثل نسبة الطلبة الذين يستخدمون الأنترانت للمشاهدة الأفلام والبرامج، اما بنسبة للطلبة الذين يستخدمون الأنترانت للعمل كانت نسبتهم 16.90%.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة أسباب أستخدم للأنترانت يعود الي التعليم بتكرار قدره 126 طالب، ونسبة مئوية 35.49% من مجموع العام، حيث هذا راجع لخصوصية العينة بحكم انتماءها للمؤسسة التعليم العالي ذات النشاط العلمي فهذا يفرض على الاستخدام العام للأنترانت من طرف الطالب هو التعلم، بسبب الحاجة إلى الوصول إلى المعلومات والموارد التعليمية المتاحة على الإنترنت، إضافة الى العديد من الأدوات والتطبيقات التعليمية المتاحة على الإنترنت، وهذا مسمح لهم بالوصول إلى مجموعة واسعة من الموارد التعليمية المفيدة بكل سهولة ويسر، لتعزيز القدرات التعليمية للطلاب وتعزيز تحصيلهم الدراسي، وتجاوز الصعوبات في تعلم اللغات الأجنبية وتحسين مهاراتهم التعليمة.

أما بنسبة، لطلبة التي تعرف استخدام للغرض الدردشة وتكوين صدقات بتكرار قدره 99 طالب ونسبة مئوية 27.90%من مجموع العام، بحكم أن الطالب اجتماعي بطبعه فالتفاعل مع الأخرين جزء منه وتكنولوجيا الاتصال اضفت على التفاعل طابع الافتراضي من خلال الوسائط الإلكترونية، وكثير من الطلبة يتوجهون اليه لتعزيز التواصل الاجتماعي وتقليل الشعور بالعزلة والوحدة، خاصة بالنسبة لطلبة الذين يجدون صعوبة في تكوين صدقات في العالم الحقيقي بسبب خجلهم وصعوبة التواصل مع الأخرين، فهو من الجانب النفسي يشعرهم بالسعادة والاستقرار النفسي وراحة أكثر في الحياة الافتراضية، من خلال التعرف على أصدقاء بثقافات مختلفة وجديدة بالنسبة لهم.

أما بنسبة، لطلبة التي تعرف استخدام للغرض العمل، بتكرار قدره 60 طالب ونسبة مئوية 16.90%من مجموع العام، حيث تعتبر ثقافة العمل عبر الأنترانت من الثقافات الجديدة التي توجها اليها

الشاب الجزائري، وبحكم الظروف الاقتصادية مثل توفير تكاليف الدراسة والاجتماعية مثل البطالة التي تفرض عليه استغلال مهاراته عبر العمل عن بعد واستخدام الطلاب للإنترنت في العمل يمثل نمطًا تكنولوجيًا اجتماعيًا ينعكس على التطور السريع للتكنولوجيا المعلومات في الجزائر.

أما بنسبة، لطلبة التي تعرف استخدام للغرض مشاهدة الأفلام والبرامج، بتكرار قدره 70 طالب ونسبة مئوية 19.71%من مجموع العام، وهذا يدخل في جانب الاستمتاع والترفيه لتخلص من ضغوطات التعليم.

جدول (14): يبين مستوي معرفة الطلبة بمجال الأمن السيبراني:

مستوي معرفة الطلبة بالأمن السيبراني	التكرار	النسبة المئوية
منخفضة	80	%22.55
متوسطة	210	%59.15
عالية	65	%18.30
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن نسبة 59.15%من الطلبة مستوي معرفتهم بالأمن السيبراني متوسطة مقابل نسبة 22.55%، مستوي معرفتهم بالأمن السيبراني منخفضة في حين أن 18.30% تمثل نسبة الطلبة مستوي معرفتهم بالأمن السيبراني عالية.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة مستوي معرفتهم بالأمن السيبراني كانت منحصرة بين مستوي المنخفض والمتوسط، بتكرار قدره 290 طالب ونسبة مئوية 81.70% من مجموع العام حيث، باعتبار المعرفة في الأمن السيبراني تركز على قدرات الطالب في تمكن من الإجراءات والتقنيات والأدوات، التي تستخدم لحماية الأنظمة الإلكترونية خاصة بأجهزتهم مثل الحاسوب والهاتف إضافة الى بياناتهم ومعلوماتهم من الهجمات الإلكترونية والتهديدات السيبرانية.

وهنالك عديد من الأسباب التي يمكن تطرق اليها فيما يخص سبب تدني مستوي معرفة في مجال الأمن السيبراني، من بينها طريقة تدريس مناهج ودروس تخصصات العلوم الإنسانية والاجتماعية في

الجامعة الجزائرية، حيث تركز على دراسة الظاهرة بحد ذاتها وتطرق الى مخاطرها في أطار النظري دون التركيز على تطوير مهارات الطالب في الحماية منها وهذا ما يأدي الى زيادة مخاطر الاختراقات السيبرانية، والهجمات الإلكترونية التي تهدد الطلبة وخاصة في ضل الاعتماد على التعليم عند بعد.

أما بنسبة الطلبة الذي مستواهم عالي في مجال المعرفة بالأمن السيبراني، كان بتكرار 60طالب ونسبة مئوية 18.30% من مجموع العام حيث، يعتبر نسبة قليلة مقارنة بالمجموع الكلي لعدد الطلبة، وهذا راجع لتمكنهم في مفاهيم الأساسية والممارسات المتعلقة بأمنهم السيبراني من خلال الاعتماد على التعليم الذاتي، في تطوير مهاراتهم في هذا المجال بحكم العديد من طلبة يعتمدون على استخدام الأنترانت، في التعلم ويخصصون وقت لمجال الأمن السيبراني ويشهد هذا المجال في سنوات الأخير أهمية بالغة بحكم التحول الرقمي الذي تشهده المؤسسات التعلمية، على مستوي العالمي والمحلي وتزيد مخاطر السيبرانية والهجمات الإلكترونية، أصبحت يفرض على الأفراد تمتع بالحيطة والحذر واستخدام الواعي لكل فيم يتعلق بالأنترانت.

جدول (15): يبين الوعي السيبراني في نظر الطلبة

الوعي السيبراني في نظر الطلبة	التكرار	النسبة المئوية
تنفيذ الأنشطة عبر الإنترنت بشكل آمن	170	%47.90
الوعي بالمخاطر الهجمات الإلكترونية	105	%29.57
حفاظ على أمن خصوصيات بياناتي الشخصية	80	%22.53
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول، أن نسبة 47.90%من الطلبة في نظرهم الوعي السيبراني تنفيذ الأنشطة عبر الإنترنت بشكل آمن، مقابل نسبة 29.57% في نظرهم الوعي السيبراني هو الوعي بالمخاطر الهجمات الإلكترونية، في حين أن نسبة 22.53% تمثل نسبة الطلبة الذين في نظرهم الوعي السيبراني حفاظ على أمن خصوصيات بياناتهم الشخصية.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة الوعي السيبراني في نظرهم هو تنفيذ الأنشطة عبر الأنترانت بشكل أمن، بتكرار قدره 170 طالب، ونسبة مئوية 47.90% من مجموع العام حيث،

وهذا بحكم تنوع الأنشطة عبر الأنترانت فمنهم من يعتمد على الأنترانت في التعلم او الدردشة او العمل او التسوق الإلكتروني، وهذا يفرض عليهم أدراك الأساليب الأمنة في أنجاز أعمالهم، من خلال تجنب دخول الي المواقع غير الأمنة او تحميل الملفات من مصادر غير موثوقة.

كمان العديد من الطلبة يعتبر أن الوعي السيبراني يستوجب الوعي بالمخاطر الهجمات الإلكترونية من وجهة نظرهم، بتكرار قدره 105 طالب، ونسبة مئوية 29.57% من مجموع العام حيث، تعد الهجمات الإلكترونية من المخاطر الكبرى التي تواجه الطلبة خاصة في عصر التكنلوجيا الحديثة، الذي جعل كل الجرائم الكلاسيكية التي كانت في العالم الحقيقي جزء من حياة الطالب في العالم الافتراضي، ويعطيها جزء كبير من وعيه السيبراني نتيجة تسليط العديد من القنوات التلفزيونية وإحصاءات الشرطة والدرك الوطني للشكوى المواطنين نتيجة العديد من الجرائم الإلكترونية التي يكنون ضحية لها، وهذه العوامل تلعب دور كبير في ادراك مخاطر الاستخدام السيئ للأنترانت.

كما العديد من الطلبة يعتبر أن الوعي السيبراني يستوجب حفاظ على أمن خصوصيات بياناتي الشخصية من وجهة نظرهم، بتكرار قدره 80 طالب، ونسبة مئوية 22.53% من مجموع العام حيث، يعتبر حفظ امن البيانات وخصوصياتها من أكبر التحديات التي يواجها الطلبة كون عديد من المخاطر يوجهها الأفراد التي لا تعطي أهمية بالغة لبياناتها الشخصية فهو جزء أساسي من الوعي السيبراني، من خلال تطبيق العديد الخطوات التي تحقق له حماية للبيانات الشخصية مثل استخدام الكلمات المرور القوية التي تجعل الهاكر يجد صعوبة في اختراق حسابتهم الشخصية إضافة الي البرامج المضادة للفيروسات والتي تكشف الثغرات في النظام المعلوماتي خاص بنظام أجهزتم في الهاتف والحاسوب.

جدول (16): الأنشطة التي يتجنبها الطلبة على الإنترنت للحافظ على أمانهم:

الأنشطة التي يتجنبها الطلبة على الإنترنت	التكرار	النسبة المئوية
الدخول إلى مو اقع غير آمنة	160	%45.07
تحميل الملفات من مصادر غير موثوقة	80	%22.53
الإفصاح عن معلوماتي شخصية	115	%32.40
المجموع	355	%100

نلاحظ من خلال هذا الجدول أن نسبة45.07%من الأنشطة التي يتجنبها الطلبة على الإنترنت للحافظ على أمانهم هي الدخول إلى مواقع غير آمنة بنسبة 45.07%، مقابل نسبة 32.40% التي تتجنب الإفصاح عن معلوماتهم شخصية، في حين أن 22.53% تمثل نسبة الطلبة الذين يتجنبون تحميل الملفات من مصادر غير موثوقة.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة يتجنبون الدخول الى المواقع الغير الأمن بتكرار قدره 160 طالب، ونسبة مئوية 45.07% من مجموع العام حيث ان المعروف عن هذه الموقع تنتشر فيها العديد من الظواهر التي تشكل خطر عليهم مثل الاحتيال الإلكتروني، الذي يمارس من خلال البريد الإلكترونية عند تسجيل في هذه المواقع حيث يطلب تزويدهم بمعلومات حساسة كجزء من سرقة البيانات، إضافة الى الفيروسات المنشرة فيه وتعود بضرر على جهاز المستخدم.

كمأن العديد من الطلبة يتجنبون الإفصاح عن معلوماتهم الشخصية بتكرار قدره 115 طالب ونسبة مئوية 32.40% من مجموع العام حيث، بحكم الخوف على الاستخدام الغير القانوني لبياناتهم مم يعرضهم الى خطر العقوبات القضائية، برغم عدم قيامهم بالفعل وهذا نتيجة للانتهاك خصوصياتهم حيث يجعل الطلبة حرصين على بيناتهم عند التفاعل الافتراضي

بإضافة الي، العديد من الطلبة يتجنبون تحميل الملفات من المصادر غير الموثوقة كونها تشكل ضرر على الأجهزة وكثير من الملفات تأدي الى، انتشار الإعلانات غير الأخلاقية والتي لا تتوافق مع قيم مجتمع وتأدي بهم الانحلال الأخلاقي، فهم بدرجة وعي كبيرة في جانب الحفاظ على أمنهم عند استخدام الأنترانت.

جدول (17): الخطوات الأساسية التي يتبعها الطلبة لتعزيز امنهم السيبر اني:

الخطوات الأساسية لتعزيز امن السيبر اني	التكرار	النسبة المئوية
تحديث البرامج الخاص بجهازي (حاسوب/الهاتف)	145	%40.84
تجنب فتح رسائل البريد المجهولة	70	%19.71
بصفة دورية (البريد الإلكتروني/مو اقع التواصل الاجتماعي) استخدام كلمات مرور قوية ومتنوعة	90	%25.35
تثبيت برامج المضادة للفيروسات (حاسوب/الهاتف)	50	%14.10
المجموع	355	100.0%

نلاحظ من خلال هذا الجدول أن 40.84% من الخطوات الأساسية التي يتبعها الطلبة لتعزيز امنهم السيبراني هي تحديث البرامج الخاص بجهاز مثل (حاسوب وللهاتف) مقابل 25.35% من نسبة الطلبة، يستخدمون كلمات مرور قوية ومتنوعة بصفة دورية بنسبة (البريد الإلكتروني/مواقع التواصل الاجتماعي) في حين أن 19.71% تمثل نسبة الطلبة الذين يتجنبون فتح رسائل البريد المجهولة، اما بنسبة للطلبة الذين يقمون بتثبيت برامج المضادة للفيروسات في (حاسوب/الهاتف) كانت نسبتهم 16.90%.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة يعززون أمنهم السيبراني من خلال تحديث البرامج الخاص بأجهزتهم بتكرار قدره 145 طالب، ونسبة مئوية 40.84% من مجموع العام حيث، يعتبر تحديث البرامج الخاص بالجهاز على اصلاح الثغرات الأمنية التي يمكن استغلالها من طرف مجرم الإلكتروني للاختراق جهاز وبيانات الطالب وهذا سلوك يحسن مستوي الأمن للجهاز عن الاتصال بالأنترانت.

بإضافة الي هذا، هنالك العديد من الطلبة يعتمدون استخدام كلمات مرور قوية ومتنوعة بصفة دورية (البريد الإلكتروني/مواقع التواصل الاجتماعي) لتعزيز أمنهم السيبراني بتكرار قدره 90 طالب، ونسبة مئوية 25.35% من مجموع العام حيث، تمنع الكلمات المرور القوية الاختراق للحسابات الشخصية للطالب عكس كلمات المرور الضعيفة، التي يجد المجرمون الإلكترونين سهولة في تجاوزها والوصول الي بيانات الطالب واستغلالها بطريقة غير قانونية فالاستخدام الدوري والمنتظم للكلمات المرور القوية والمتنوعة، يحسن من مستوي الأمن السيبراني وهو يعكس السلوك الواعي للطالب الذي يتماشى مع معاير الامتثال لمتطلبات الأمنية.

ومع ذلك، هنالك العديد من الطلبة يجنبون فتح رسائل البريد المجهولة، بتكرار قدره 70 طالب ونسبة مئوية 19.71% من مجموع العام حيث، تثير الرسائل المجهول قلق طلبة بحكم ما تحمله من مخاطر كبيرة عليهم، مثل الاحتيال والتهديد والانتهاكات القانونية لخصوصياتهم حيث يفرض عليهم حذفها وتجنب فتحها.

وفي الأخير، هنالك العديد من الطلبة تثبيت برامج المضادة للفيروسات في، (حاسوب والهاتف) بتكرار قدره 50 طالب ونسبة مئوية 14.10% من مجموع العام حيث، هذا نوع من البرامج له دور كبير للكشف المبكر عن الفيروسات في الجهاز، وحذفها وبهذا لا يكون اختراق لبيانات الطالب ويحقق من خلالها الحماية الشاملة لجهازهم.

جدول (18): أهمية الوعي السيبراني في نظر الطلبة:

أهمية الوعي السيبراني	التكرار	النسبة المئوية
الحفاظ على سلامة معلوماتي	85	%23,94
الوقاية من الهجمات والجرائم الإلكترونية	165	%46,47
زيادة أماني عند استخدام الإنترنت	105	%29,59
المجموع	355	%100

نلاحظ من خلال هذا الجدول أن 46,47%من الطلبة يعتبرون أهمية الوعي السيبراني في نظر هي الوقاية من الهجمات والجرائم الإلكترونية مقابل 29,59% هي زيادة أمانهم عند استخدام الإنترنت في حين أن، 23,94% تمثل نسبة الطلبة الذين يعتبرون أهمية الوعي السيبراني في نظر الحفاظ على سلامة معلوماتهم.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة يعتبرون أهمية الوعي السيبراني في الوقاية من الهجمات والجريمة الإلكترونية بتكرار قدره 165 طالب، ونسبة مئوية 46,47% من مجموع العام حيث، بحكم أنها الظاهرة أصبحت تغزو الفضاء الافتراضي وكل المستخدمين المشتركين في المواقع التواصل، يواجهون خطر الوقع ضحية لنوع من الهجمات الإلكترونية او لجريمة السيبرانية، لهذا فهم يعتبرون أن زيادة وعيهم السيبراني يحقق لهم شرط الأساسي في تحقيق الحماية الشاملة من خطر الجريمة.

إضافة الى ذالك، فعديد من الطلبة يعتبرون ان زيادة الأمن السيبراني عندهم مربوط بدرجة وعيهم بتكرار قدره 105 طالب، ونسبة مئوية 29,59% من مجموع العام حيث، ان اتخاذ قرارته اللزمة عند مواجهة أي خلال تقني نتيجة لهجوم سيبراني يكون بدرجة الوعي بالمهارات الأساسية، التي من خلالها تكون درجة تنبؤه بأخطر عالية ويتخذ سلوك السليم لحل المشاكل التي توجهه.

وفي الأخير، يشكل الحفاظ على سلامة معلومات في الوقع الافتراضي بنسبة للطالب جزء أساسي في أهمية الوعي السيبراني بتكرار قدره 85 طالب، ونسبة مئوية 23,94% من مجموع العام حيث، نتيجة لتحول الرقمي الذي أصبح تبادل أسهل الى أنا استغلالها وانتهاكها يشكل خطر بنسبة لهم فهم يولون أهمية لها وهي جزء أساسي بنسبة لوعيهم السيبراني عند استخدام الأنترانت.

جدول (19): مستوي معرفة الطلبة بالجريمة الالكترونية:

مستوي معرفة بالجريمة الالكترونية	التكرار	النسبة المئوية
منخفضة	78	%22,00
متوسطة	167	%47,00
عالية	110	%31,00
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن47,00%من الطلبة مستوي معرفتهم بالجريمة الالكترونية متوسطة، مقابل 22,00% مستوي معرفتهم بالجريمة الالكترونية منخفضة في حين أن 31,00% تمثل، نسبة الطلبة الذين مستوي بالجريمة الالكترونية عالية.

نستنتج من خلال معطيات الجدول، ان أكبر نسبة من الطلبة ليهم معرفة متوسط وعالية للجريمة الإلكترونية بتكرار قدره 167 طالب، ونسبة مئوية 47,00% من مجموع العام، وهذا بنسبة لطلبة لمعرفهم بالجريمة الإلكترونية متوسطة، اما بنسبة لطلبة الذي كان مستوي معرفتهم للظاهرة الجريمة الالكترونية عالي فقد قدر بتكرار قدره 110 طالب، ونسبة مئوية 31,00% من مجموع العام حيث، تزايد الاعتماد على تكنولوجيا والإنترانت في الحياة اليومية للطالب في العديد من الجوانب مثل التعلم والعمل والدردشة والتسوق الرقمي، فعديد من الأعمال التي كانت تمارس في الحياة الحقيقة قد انتقلت الي الحياة الافتراضية، ونتيجة هذا التحول سوف تتطور تقنيات ارتكاب الجريمة، ولذلك يجب على الطلبة بالمعرفة بالجريمة الإلكترونية من خلال ان يتتابعوا تطورات الظاهرة ويتعلموا كيفية مواجهتها من كل جوانب القانونية و التقنية و تطوير مهاراتهم مم يعود عليهم بالإجاب لزيادة أمنهم السيبراني، وبحكم أن العينة هم طلبة العلوم

الاجتماعية والإنسانية فهم لديهم معرفة بالظاهرة بحكم من الظواهر الكبرى التي تهدد الأمن الدولي وتهتم بدراستها كل التخصصات الإنسانية.

أما بنسبة لطلبة الذي كان مستواهم منخفض حول معرفة حول الجريمة الإلكترونية بتكرار قدره 78 طالب وبنسبة مئوية قدرت ب 22,00% من مجموع العام، وهذا راجع أولا لتخصصات مثل التاريخ وعلم المكتبات التي طلبتها وتخصصهم لا يهتم بدراسة ظاهرة الجريمة إضافة الي هنالك عديد من عوامل الاجتماعية والشخصية التي تأثر على معرفتهم على الظاهرة مثل الاستخدام القليل للأنترانت، واهتمام الطالب بالحياة الحقيقية على التفاعل الافتراضي تساهم في تقليل معرفته بالظاهرة.

جدول (20): أكثر الجرائم الالكترونية التي يلاحظها الطلبة عند استخدامك الأنترانت:

أكثر الجرائم الالكترونية التي يلاحظها الطلبة	التكرار	النسبة المئوية
التهديد والمضايقة مثل(قرصنة/التنمر/التخويف/الابتزاز)	84	%23,66
القذف والسب مثل (ترويج أخبار الكاذبة/تقليل من الاحترام/مساس بكرامة)	99	%27,90
الجرائم غير الأخلاقية مثل (مواقع غير الأخلاقية/صور جنسية)	96	%27,04
الجرائم المالية (سرقة أرقام بطاقة البنكية/احتيال عند تسوق الإلكتروني)	76	%21,40
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن 27,90% من أكثر الجرائم الالكترونية التي يلاحظها الطلبة عند استخدام الأنترانت، هي القذف والسب مثل (ترويج أخبار الكاذبة/تقليل من الاحترام/مساس بكرامة)، مقابل 27,04%من الطلبة يلاحظون الجرائم غير الأخلاقية مثل (مواقع غير الأخلاقية/صور جنسية)، في حين أن 23,66% تمثل نسبة الطلبة الذين يلاحظون جرائم التهديد والمضايقة مثل(قرصنة/التنمر/التخويف/الابتزاز)، اما الطلبة الذين يلاحظون الجرائم المالية مثل (سرقة أرقام بطاقة البنكية/احتيال عند تسوق الإلكتروني) كانت نسبتهم 21,40%.

نستنتج من خلال معطيات الجدول، أن من أكثر الجرائم الالكترونية التي يلاحظها الطلبة عند استخدامهم الأنترانت اذ جاءت جرائم القذف والشتم بتكرار قدره 99 طالب وبنسبة مئوية قدرت ب27,90% من مجموع العام، حيث عرف هذا نوع من الجرائم أنتشار المواقع التواصل الاجتماعي ويشكل العديد من الأضرار الاجتماعية والنفسية على الضحية وتتنوع صوره وأشكاله مثل ترويج الاخبار الكاذبة وتقليل من

الاحترام الأفراد ومساس بالكرامة وكل هذه السلوكيات مخالفة للقانون التشريعي الجزائري، وتعتبر من السلوكيات التي اكتسبها المجرمين من الواقع المادي و يمارسونها في الواقع الافتراضي ومم زادا في أنشرها هي التقنيات التواصل الحديثة وغياب الرقابة، كما نلحظ من الجرائم المنتشرة هي جرائم الغير الأخلاقية التي كانت بتكرر قدره 96 طالب وبنسبة مئوية قدرت ب27,04% من مجموع العام، التي كانت تمارس في القديم من خلال تأثير جماعة الرفاق او المحيط الذي يعيش فيه الفرد الى أن مع تعدد الوسائط الالكترونية أصبحت هناك جهات خاص من المجرمين دورهم هو مساس بقيم الأخلاقية للفرد من خلال أرسال له صور وروابط إلكترونية يتم دعوته، الى مشاهدة أفلام إباحية او صور جنسية وتستهدف فئة المراهقين الذين يعتبرون فئة في قيد تنشئة الاجتماعية وهي مستقبل المجتمع.

بإضافة الي، هذا أصبح يعاني مستخدمي الأنترانت من التهديد والمضايقة بحكم قابلية الفرد للملاحظة من طرف المجرمين و خصوصيته التي تميزه عن البقية المستخدمين مثل مشاهير السوشيل ميديا، التي تعاني من قرصنة حساباتهم والتنمر على حياته الشخصية التي يشاركها مع المتابعين الخاص بهم من خلال تخويفهم وابتزازهم، حيث أن المجتمع الجزائري يستهلك الفضيحة المنشورة على مواقع التواصل الاجتماعي والتي تلقي تفاعل كبير مم يساهم في أنشارها بسرعة وتكون قابلة لملاحظة عند الجميع، وجاءت جرائم التهديد والمضايقة بتكرار قدره 84 طالب وبنسبة مئوية قدرت ب23,66% من مجموع العام، يقابلها جرائم المالية بتكرار قدره 76 طالب وبنسبة مئوية قدرت ب21,40% من مجموع العام، وهذا نتيجة التحول الرقمي الذي شهدته المؤسسات الجزائرية، واعتماد على الدفع الالكتروني والتسوق عبر الأنترانت ممادي للانتشار جرائم مثل سرقة أرقام بطاقة البنكية واحتيال عند تسوق الإلكتروني.

جدول (21): وقع الطلبة في الجرائم الالكترونية أثناء استخدام الأنترانت

وقع في الجرائم الالكترونية أثناء استخدام الأنترانت	التكرار	النسبة المئوية
تعرضت الى جريمة واحدة	172	%48,45
تعرضت الى من جريمتين الى ثلاث جرائم	118	%33,25
أكثر من أربع جرائم	65	%18,30

المجموع	355	100.0%

نلاحظ من خلال هذا الجدول أن48,45% من الطلبة الذين وقع ضحايا للجريمة الالكترونية مرة واحدة، مقابل 33,25% من الطلبة الذين وقع ضحايا للجريمة الالكترونية من جريمتين الى ثلاث جرائم، في حين أن 18,30% تمثل نسبة الطلبة الذين وقع ضحايا للجريمة الالكترونية أكثر من أربع جرائم.

نستنتج من خلال معطيات الجدول أن أكثر الطلبة وقع ضحية للجريمة الإلكترونية عند استخدامهم الأنترانت متوسط جريمة إلكترونية واحدة بتكرار قدره 172 طالب وبنسبة مئوية قدرت ب48,45% من مجموع العام، وهنالك العديد من العوامل التي تساهم في وقع الطلبة في جريمة إلكترونيه حيث نلاحظ، ان أكبر نسبة من الطلبة مستوي معرفتهم بالأمن السيبراني كانت منحصرة بين مستوي المنخفض والمتوسط، فبعتبار المعرفة في الأمن السيبراني تركز على نحسين قدرات الطالب في تمكن من الإجراءات والتقنيات والأدوات، التي تستخدم لحماية الأنظمة الإلكترونية خاصة بأجهزتهم مثل الحاسوب والهاتف إضافة الى بياناتهم ومعلوماتهم من الهجمات الإلكترونية والتهديدات السيبرانية.

كمأن، أكبر نسبة من الطلبة تعرف استخدام أكثر من 3ساعات للأنترانت بتكرار قدره 220 طالب، ونسبة مئوية 61.97% من مجموع العام حيث، نتيجة للحاجة إلى إنجاز الأعمال، الأكاديمية والأبحاث مقدمة من طرف الأساتذة إليهم في إطار تكوينهم في طورين لسانس وماستر، ويعتمد هذا الأمر على نوعية التخصص مثل تخصصات العلوم الإنسانية والاجتماعية والتي، تعرف توافر مقالات العلمية والكتب ذات المصادر الإلكترونية اللازمة لإنجاز العمل البحثي، كما أصبحت عديد من الامتحانات التي يتم أنجازها عن بعد في الجامعة الجزائرية والتي تفوق ثلاث ساعات للاختبار مستوي الطالب وتفرض عليه استخدام الأنترانت.

وبهذا فالاستخدام الأنترانت لمدة كبيرة ومستوي متوسط وضعيف معرفة بالأمن السيبراني والجريمة الإلكترونية يساهم في وقوع الطالب ضحية لجريمة الالكترونية وكلما تعددت مرات الوقوع ضحية في الجريمة يتم تقيمه حسب مهارات الطالب في تعامل مع الهجمات الإلكترونية.

جدول (22): الجريمة الالكترونية التي تعرضتا لها الطلبة

الجريمة الالكترونية التي تعرضتا لها	التكرار	النسبة المئوية
قرصنة حساب التوصل الاجتماعي خاص بك	89	%25,00
انتحال شخصيتك (سرقة بياناتك او صورك)	75	%16,00
الاحتيال عليك عند التسوق الإلكتروني	45	%15,00
تعرض لشتم والتهديد	97	%27,00
أرسال صوروروبط لمو اقع غير أخلاقية	58	%17,00
المجموع	355	100.0%

نلاحظ من خلال هذا الجدول أن 27,00% من أكثر الجرائم الالكترونية التي تعرض لها الطلبة عند استخدام الأنترانت هي تعرض لشتم والتهديد مقابل 25,00% منهم تعرضوا للقرصنة حساب التوصل الاجتماعي خاص بهم، في حين أن 16,00% تمثل نسبة الطلبة الذين تعرضوا الى ارسال صور وروبط لمواقع غير أخلاقية لهم، اما بنسبة للطلبة الذين تعرضوا للجرائم انتحال شخصيتك، مثل (سرقة بياناتك او صورك) 17,00% مقابل 16,00% من الطلبة تعرضوا الاحتيال عليه عند التسوق الإلكتروني.

نستنتج من خلال معطيات الجدول أن أكثر الطلبة، وقع ضحية للجريمة الإلكترونية عند استخدامهم الأنترانت و كانت من بين الجرائم هي الشتم والتهديد بتكرار قدره 97 طالب وبنسبة مئوية قدرت ب27,00% من مجموع العام، وهذه تدخل في عدم احترام أراء الأفراد في عملية التفاعل في الفضاء الرقمي خاصة في التعليق على الصور والفيديوهات حيث تنتشر ظاهرة الشتم والتهديد نتيجة اختلاف وجهات النظر، بإضافة الى نقص التربية وتنشئة اجتماعية والوعي السليم في التفاعل الافتراضي وعدم تمتع بثقافة المواطنة الرقمية وغياب معرفة بأن شتم والتهديد يعتبر جريمة الكترونية ونقص رفع شكوي عند السلطات الأمنية يزيد من أنتشارها.

أضافة الى، جرائم قرصنة حساب التوصل الاجتماعي خاص بطلبة تكون نتيجة استخدامهم لكلمات مرور ضعيفة، يسهل لمجرم الإلكتروني اختراقها، فاستعمال نفس كلمة المرور في نفس المواقع التي يستعملها في التواصل الاجتماعي سلوك غير واعي مم يضعف سلامة أمنه عند استخدام الأنترانت.

كمأن، احتيال على الطالب مثل انتهاك خصوصياته وسرقة صوره، وإعادة استخدامها في حسابات أخري تحمل أسمه هذا راجع لنشر صوره مع الغرباء وعدم حمايتها فهذه سلوكيات يستوجب تجنبها، خاصة إذا كان حساب الشخصي عام فيكون سهل الاستهداف من طرف المجرمين أضافة الى، احتيال عند التسوق الإلكتروني، حيث يهم العديد من التجار الوهمين الطلبة بتوفر سلع ويقدم لهم خدمة غير حقيقة وثقة فيه تأدي بوقع الى هذا نوع من الجرائم.

جدول (23): أسبقية رفع شكوى عند الشرطة بسبب تعرض طلبة للجريمة الالكترونية:

أسبقية رفع شكوى عند الشرطة	التكرار	النسبة المئوية
نعم	70	% 19,71
لا	285	% 80,29
المجموع	355	%100

نلاحظ من خلال هذا الجدول أن80,29% من الطلبة الذين وقع ضحايا للجريمة الالكترونية ولم يرفعوا شكوى عند الشرطة، مقابل19,71%من الطلبة الذين رفعوا شكوى عند الشرطة.

نستنتج من خلال معطيات الجدول أن أكثر الطلبة وقع ضحية للجريمة الإلكترونية عند استخدامهم الأنترانت لم يرفعوا شكوي عند الشرطة بتكرار قدره 285 طالب وبنسبة مئوية قدرت ب80,29% من مجموع العام، وهذا يعود لخصوصية الجريمة الإلكترونية بحد ذاتها حيث هنالك العديد من الجرائم السيبرانية التي يصعب تحديد هوية مرتكبها، في الفضاء الافتراضي أضافة الى احترافية المجرم الالكتروني الذي يستعمل تقنيات المتطورة للاختفاء الأثر الفعل الإجرامي، التي تصعب الإجراءات القانونية اللازمة فمثل القرصنة الإلكترونية و الاحتيال و الابتزاز والتحرش ممارس في الفضاء السيبراني تطلب هذه الجرائم مهارات تقنية متقدمة، وقد يكون من الصعب تحديد المتهمين في هذه الجرائم.

أما بنسبة، للأشخاص الذين يستعملون هويتهم الحقيقية في ممارسة الجريمة الإلكترونية ويكونون معرفون من طرف الضحية، يسهل اتخاذ إجراءات القانونية اللازمة من طرف الشرطة لهذا نجد ان الطلبة الذين وقع ضحية للجريمة الإلكترونية، عند استخدامهم الأنترانت ورفعوا شكوى عند الشرطة كانو بتكرار قدره 70 طالب وبنسبة مئوية قدرت ب 19,71% من مجموع العام.

جدول (24): أسباب عدم رفع شكوى عند الشرطة بسبب تعرض طلبة للجريمة الالكترونية:

أسباب عدم رفع شكوى عند الشرطة	التكرار	النسبة المئوية
عدم معرفتي بأن فعل ممارس يعتبر جريمة	85	%29,82
ليس لدي معرف بقانون الجريمة الإلكترونية	120	%42,10
غياب الدليل ومجرم مجهول	80	%28,08
المجموع	285	%100

نلاحظ من خلال هذا الجدول، أن42,10% من الطلبة الذين وقع ضحايا للجريمة الالكترونية ولم يرفعوا شكوى عند الشرطة كان سبب عدم معرفتهم بقانون الجريمة الإلكترونية مقابل 29,82% من الطلبة الذين كان سبب عدم معرفتهم بأن فعل ممارس يعتبر جريمة في حين أن 28,08% تمثل نسبة الطلبة الذين كان سبب غياب الدليل ومجرم مجهول.

نستنتج من خلال هذا ان الطلبة الذين وقع ضحية للجريمة الإلكترونية عند استخدامهم الأنترانت، ولم يرفعوا شكوي عند الشرطة بتكرار قدره 285 طالب وبنسبة مئوية قدرت ب80,29% من مجموع العام، حيث نجد أسباب عدم التبليغ متنوع أضافة للأسباب المعروفة عن الجريمة الإلكترونية التي يصعب تحديد هوية مرتكبها، في الفضاء الافتراضي أضافة الى احترافية المجرم الالكتروني الذي يستعمل تقنيات المتطورة للاختفاء الأثر الفعل الإجرامي التي تصعب الإجراءات القانونية، حيث نجد عدم معرفة الطالب بقانون الجريمة الإلكترونية كان بنسبة مئوية 42,10% من بين الأسباب التي تمنعه من التبليغ وهذا ما يأثر علي وعيه القانوني لظاهرة الإجرامية من جانب أخر، يجعله في وضعية خطرة عند استخدام الأنترانت ويكون ضحية للجرائم أخري، ومن أسباب هي غياب تدريس القانون في مناهج تخصصات كلية العلوم الاجتماعية والإنسانية، إضافة الى عزوف الطالب عن الملتقيات الوطنية والدولية التي تنظمها الجامعة عن موضوع الجريمة الإلكترونية.

كمأننا نجد، من بين الأسباب التي تمنعه من التبليغ هي عدم معرفة بأن السلوك الممارس هو جريمة إلكترونية والتي كانت بنسبة مئوية 29,82% تقبلها نسبة 28,08%عدم وجود دليل والمستخدم مجهول بنسبة للطلبة، فهناك العديد من الطلبة مزال يركز على السلوك الكلاسيكي للجريمة وهذا راجع

لخصوصية فئة العينة البحثية، التي تعتبر من فئة الشباب التي تراوح أعمارهم بين 17 سنة الى 26 سنة حيث أن فئة هذه تهتم بالمواضيع التي تلفت انتباههم وتحسن حياتهم اليومية فهم في مرحلة التكوين خاصة انتقال من التعليم في الأطوار الثلاثة ابتدائي متوسط وثانوي، الى الدارسات العليا هنالك فروقات كبيرة بين برنامجي التعليم ولهذا نجد أن العديد من الجرائم في الوقاع المادي تكون أسبابها في الواقع الافتراضي نتيجة لشتم او استفزازا.

جدول رقم (25): العوامل التي تأدي الى وقع في جريمة الإلكترونية من منظور الطلبة:

العوامل التي تأدي الى وقع في جريمة الإلكترونية	التكرار	النسبة المئوية
الثقة في الغرباء	49	%13,80
غياب المعرفة بالجريمة الإلكترونية	64	%18,02
تصفح المو اقع الغير الامنة	58	%16,33
غياب المعرفة بمجال الأمن السيبر اني	78	%22,00
غياب لمعرفة بقو انين التشريعية الجز ائرية للجريمة الإلكترونية	106	%29,85
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن 29,85% من العوامل التي تأدي الى وقع في جريمة الإلكترونية من منظور الطلبة هي غياب لمعرفة بقوانين التشريعية الجزائرية للجريمة الإلكترونية، مقابل 22,00%من الطلبة الذين يعتبرون غياب المعرفة بمجال الأمن السيبراني هي التي تأدي الى وقوع ضحية للجريمة الالكترونية، في حين أن 18,02% تمثل نسبة الطلبة الذين يعتبرون غياب المعرفة بالجريمة الإلكترونية هو سبب الوقوع ضحية للجريمة اما بنسبة للطلبة الذين يعتبرون تصفح المواقع الغير الامنة، هو سبب فكانت نسبتهم 16,33%مقابل 13,80% من الطلبة الذين يعتبرون الثقة في الغرباء، هي عامل من عوامل الوقع ضحية في الجريمة الالكترونية.

نستنتج من خلال معطيات الجدول ان من العوامل التي تأدي الى الجريمة الإلكترونية من منظور الطلبة غياب لمعرفة بقوانين التشريعية الجزائرية للجريمة الإلكترونية جاء بتكرار قدره 106 طالب وبنسبة مئوية قدرت ب29,85% من مجموع العام، يؤدي غياب المعرفة بقانون الجريمة الإلكترونية إلى تعرض الطلبة للعديد من المخاطر الأمنية على الإنترنت، بما في ذلك الاختراقات الإلكترونية وسرقة البيانات

الشخصية الخاصة بهم والمعلومات الحساسة والاحتيال الإلكتروني والبرمجيات الخبيثة والاعتداءات الإلكترونية الأخرى، يمكن أن يؤدي الجهل بقوانين الجريمة الإلكترونية، إلى ارتكاب جرائم دون قصد عن طريق القيام بأنشطة غير قانونية بدون معرفة أنها تشكل جرائم، مما يؤدي في النهاية إلى تبعات قانونية وأضرار اقتصادية و اجتماعية وسمعة سيئة للطلبة.

أضافة الى ذالك، غياب المعرفة بمجال الأمن السيبراني يأدي الى إلى تعرض الطلبة للعديد من المخاطر الأمنية على الإنترنت، حيث يزداد التهديد السيبراني باستمرار ويصبح أكثر تطورا وتعقيدا بنسبة لهم جاء بتكرار قدره 78 طالب وبنسبة مئوية قدرت ب 22,00% من مجموع العام، ومن بين هذه المخاطر، نجد كل من اختراق الحسابات الإلكترونية لطلبة وأجهزتهم المتصلة بالأنترانت مثل الهواتف وحواسيب، مما يهدد تحقيق السلامة والامن السيبراني عند استخدام الأنترنت.

كمأن، يمكن للغرباء في الواقع الافتراضي أن يلعبوا دورًا في الجريمة، حيث يمكن للمهاجمين استخدام الهوية المزيفة والتظاهر بأنهم أشخاص آخرون للوصول إلى بيانات حساسة الخاصة بالطلبة أو القيام بأنشطة غير قانونية تهددهم، ومن الممكن أن يتسبب الثقة الزائدة في الغرباء في الواقع الافتراضي في إفساد الطلبة وخصوصية بياناتهم وتعريضهم للخطر مثلها مثل تصفح المواقع الغير الأمنة، التي يستخدمها المجرمون لارتكاب جرائم الإنترنت كمواقع التصيد الاحتيالية، والتي تشمل رسائل البريد الإلكتروني المزيفة والتي تستهدف الحصول على معلومات حساسة من المستخدمين عن طريق تزييف هوية معروفة، والمواقع الغير الآمنة التي توفر خدمات المال عبر الإنترنت، والتي تستخدم لاستنزاف أموال المستخدمين بطرق غير شرعية.

لهذا يستوجب على الطلبة تنمية معرفتهم حول الجريمة الإلكترونية، من خلال المعرفة بخصائص الظاهرة في الجانب المعرفي والقانوني، إضافة الى جانب المخاطر التي مكنهم من تجنب الوقع ضحية حيث

أن الوعي بها يجعل الطالب يختار السلوك الواعي في تحديد الحماية للزمة لمواجهة الهجمات السيبرانية، وتهديداتها ويحقق مستوي عالي من الأمن عند أستخدم الأنترنت.

جدول (26): حلول لتنمية الوعي السيبراني للجريمة الالكترونية في الوسط الجامعي في نظر الطلبة

حلول لتنمية الوعي السيبراني للجريمة الالكترونية	التكرار	النسبة المئوية
توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني	98	%27,60
تشجيع الإبلاغ عن الحوادث السيبرانية	102	%28,73
تنظيم حملات التوعية حول الوعي السيبراني والجريمة الإلكترونية	78	%21,97
تشجيع الطلبة على حضور الملتقيات الوطنية والدولية حول ظاهرة الجريمة الإلكترونية والوعي السيبراني	77	%21,70
المجموع	355	%100.0

نلاحظ من خلال هذا الجدول أن 28,73% من حلول لتنمية الوعي السيبراني للجريمة الالكترونية في الوسط الجامعي في نظر الطلبة هي تشجيع الإبلاغ عن الحوادث السيبرانية مقابل 27,60% من الطلبة توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني في حين أن 21,97% تمثل نسبة الطلبة الذين تنظيم حملات التوعية حول الوعي السيبراني والجريمة الإلكترونية اما بنسبة للطلبة الذين تشجيع الطلبة على حضور الملتقيات الوطنية والدولية حول ظاهرة الجريمة الإلكترونية والوعي السيبراني قدرت ب 21,70%.

نستنتج من خلال معطيات الجدول أن هنالك العديد من العوامل التي لها دور في تنمية الوعي السيبراني للجريمة الإلكترونية ومن بين هذه الحلول من وجهة الطلبة هي تشجيع على الإبلاغ عن الحوادث السيبراني الذي كان بنسبة مئوية 28,73% إضافة الى توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني التي كانت بنسبة مئوية 27,60%، فتبليغ عن الهجمات السيبرانية من طرف الطلبة يساعد على تحديد نوعية الهجمات التي تعرض لها والهدف منها والمخاطر الناتجة عنها من خلال تحليلها وتقييم الأضرار التي تسببها، وبالتالي يمكن اتخاذ الإجراءات اللازمة للحد من أضرارها.

أضافة الى ذالك، نجد أن تنظيم حملات التوعية حول الوعي السيبراني والجريمة الإلكترونية الذي كان بنسبة مئوية 21,97% إضافة الى تشجيع الطلبة على حضور الملتقيات الوطنية والدولية حول ظاهرة الجريمة الإلكترونية والوعي السيبراني الذي كان بنسبة مئوية 21,70% تعتبر من العوامل التي يعتبرها

الطلبة جزاء أساسيا في تنمية وعيهم حول الوعي السيبراني للجريمة بحكم أن للتوعية حول ظاهرة الجريمة الإلكترونية من خلال حضور الملتقيات الوطنية والدولية التي تنظمها الجامعات الجزائرية طوال السنة الجامعية، واستفادة من نتائج البحثية للباحثين والأساتذة وأهل الاختصاص حول الظاهرة و عمل بتوصياتهم في لتحقيق مستوي عالي من الأمن عند استخدام الأنترنت.

3.2 **عرض وتحليل الجداول المتعلقة بالسؤال الثاني** :ما درجة الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة؟

جدول (27): مستوى الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية

الرقم	الرتبة	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	1	أحرص على بياناتي الشخصية وعدم مشاركتها مع الغرباء	3,9859	1,14602	مرتفعة
2	5	اعتبر الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة	3,8479	,97393	مرتفعة
3	18	اخشي على بياناتي الشخصية من انتهاكات الامن السيبراني	3,7211	1,13917	مرتفعة
4	6	لدي دراية بأهمية الحفاظ على السرية والخصوصية في البيانات الشخصية الحساسة	3,4817	1,06912	متوسطة
5	17	اتتبع ممارسات أمان السيبراني الجيدة مثل تجنب فتح رسائل البريد الإلكتروني غير المعروفة	3,4535	1,02509	متوسطة
6	16	لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الأنترنت	3,1690	,91420	متوسطة
7	2	أقوم بتحديث نظام التشغيل بصورة دورية	3,1549	,99785	متوسطة
8	9	لدي اطلاع واسع على الجرائم والهجمات السيبرانية	3,1155	1,22620	متوسطة
9	7	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل موافقة	3,1155	1,23309	متوسطة
10	15	استخدم في جهازي تقنية التحقيق الثنائي	3,0732	1,11752	متوسطة
11	3	أستخدم جدار الحماية على جهاز الحاسوب وشبكة الخاص بي	2,9324	1,02011	متوسطة
12	14	.أستخدم برنامج للحماية من الفيروسات بصورة مستمرة	2,9127	1,14770	متوسطة
13	11	تبادل معلومات مع الطلبة حول التهديدات السيبرانية	2,9042	1,41296	متوسطة
14	12	تنظيم حملات توعوية حول التهديدات السيبرانية ينمي الوعي السيبراني لطلبة	2,8535	1,36376	متوسطة
15	10	تنمي الوعي السيبراني لطلبة التطلع على اخر الاخبار التي تخص مجال الامن السيبراني	2,7324	1,16393	متوسطة
16	4	لدي إلمام بمفهوم الوعي السيبراني	2,7268	,86765	متوسطة
17	8	لدي معوقات شخصية تمنعني من تحقيق الوقاية والامن السيبراني	2,3239	1,08891	متوسطة
		الدرجة الكلية للوعي السيبراني	**3,1609**	**1,15344**	**متوسطة**

يبين الجدول رقم (27) أن درجة الوعي السيبرانيي لدى طلبة كلية العلوم الإنسانية و الاجتماعية، من وجهة نظرهم، جاءت متوسطة، بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344)، وقد تراوحت المتوسطات الحسابية ما بين (3,9859-2,3239)، حيث جاءت الفقرة رقم (17) والتي تنص على: "

أحرص على بياناتي الشخصية وعدم مشاركتها مع الغرباء" في المرتبة الأولى وبمتوسط حسابي بلغ (3,9859)، بينما جاءت الفقرة رقم (8) والتي تنص على:" لدي معوقات شخصية تمنعني من تحقيق الوقاية والامن السيبراني" بالمرتبة الأخيرة وبمتوسط حسابي بلغ (2,3239). وبلغ المتوسط الحسابي للمجال ككل (3,1609).

نستنتج من خلال معطيات الجدول أن الوعي السيبراني لطلبة كان متوسطة بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344)، ويتم تقيم الوعي السيبراني من خلال ثلاث نقاط أساسية المعرفة بمفاهيم الوعي السيبراني، وأساليب الحماية وسبل تعزيز الوعي السيبراني حيث نلاحظ، أن الطلبة يحرصون على بيناتهم الشخصية ولا يشاركونها مع الغرباء عند أستخدم الأنترانت، وهذا نتيجة لمعرفة خطورة أنتهك غير القانوني للخصوصية بياناتهم الذي يأدي بهم الى عقوبات من طرف العدالة، حيث كان درجة العبارة رقم 17 مرتفعا بمتوسط حسابي (3,9859).

إضافة الى هذا فهم يدركون أن الوعي السيبراني جزاء أساسيا من أستخدم الأنترانت للآن كلما كان وعيهم مرتفع تجاها المخاطر السيبرانية، والتهديدات الناتجة عن الاستخدام غير الواعي للمواقع التواصل الاجتماعي، وتحميل الملفات من المواقع الغير الأمنة الذي يأدي بأضرار تقنية بنسبة للجهاز الحاسوب والهاتف التي تساهم في فقدان الطالب لبياناته الشخصية نتيجة الانتهاكات الأمن السيبراني الممارسة من طرف المجرم الالكتروني على الضحية لهذا نلاحظ ان كل من الفقرة رقم 1، التي تنص " اعتبر الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة " و6 الفقرة رقم التي " اخشي على بياناتي الشخصية من انتهاكات الامن السيبراني " بدرجة مرتفعة ومتوسطين حسابيين (3,8479) و(3,7211) على التوالي.

وبهذا نلاحظ ان درجة وعيهم السيبراني، كان مرتفعا في جانب أدراكهم بمفهوم الوعي السيبراني وعلاقته باستخدام الأنترانت، اما من جانب تعزيز الأمن السيبراني فهم يركزون على حفاظ على خصوصية بياناتهم الشخصية.

إضافة الى هذا نستنتج أن عديد من العبارات كانت درجتها متوسطة، حيث نلاحظ كان تتبعهم للممارسات الأمن السيبراني خاص في جانب رسائل البريد الإلكتروني،ومعرفتهم بمخاطر تنزيل البرامج والملفات من الأنترنت، مما يجعلهم قابلين للتعرض للهجمات السيبرانية خاصة وان درجة عبارة رقم 9 " أقوم بتحديث نظام التشغيل بصورة دورية " وعبارة رقم 7" لدي اطلاع واسع على الجرائم والهجمات السيبرانية " كانت متوسطة وهذا ميادي بالطالب الى عدم تحقيق أمنه الشامل عند استخدام الأنترانت ومن خلال هذا يستوجب تركيز على تطوير مهارات الطلبة في جانب الأساليب الحماية من خلال التوعية، وورشات التدريب حتي يتمكن الطالب من مواجه أي خلال تقني يتعرض اليه جهازه.

ومن خلال مقارنة نتائج درجة وعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة مع دراسة حمد بن حمود السواط وآخرون (2020) ،لقد اختلفت مع درجة الوعي بالأمن السيبراني لدى تلاميذ المرحلتين الابتدائية والمتوسطة، بمدينة الطائف حيث نجد الدرجة الكلية للوعي بمجال حماية الأجهزة الإلكترونية ومجال التعامل، مع أمن المتصفح عالي جدا أضافة الى نتائج دراسة ايمان عبد الفتاح عبابنه (2022) لقد اختلفت مع درجة الوعي بالأمن السيبراني لدى وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن، حيث نجد الدرجة الكلية للوعي بالأمن السيبراني لدى معلمات اللغة العربية للمرحلة الثانوية عالية، أما بنسبة لدراسة عبد الله بن حجاب القحطاني (2022) لقد اختلفت مع درجة الوعي بالأمن السيبراني لدى ذوي الإعاقة البصرية في المملكة العربية السعودية، حيث كانت درجة وعيهم بمفاهيم الوعي الأمن السيبراني متوسطة ومرتفعة بنسبة الوعي بتطبيقات الأمن السيبراني وسبل تعزيز الأمن السيبراني.

4.2 **عرض وتحليل الجداول المتعلقة بالسؤال الثالث:** ما درجة وعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة؟

جدول (28): مستوى الوعي بالجرائم الإلكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية.

الرقم	الرتبة	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	1	الجريمة الإلكترونية هي نتاج عن الانتشار الواسع للأنترانت ووسائط الإلكترونية	4,3718	,83855	مرتفعة
2	5	كل ابتزاز او سرقة بيانات في الواقع الافتراضي يعتبر جريمة الكترونية	4,1634	1,00637	مرتفعة
3	18	تسبب الجريمة الالكترونية أضرار بممتلكات الشخصية والمؤسسات الدولة العمومية والخاصة	3,8225	1,00538	مرتفعة
4	6	الجريمة الالكترونية هي كل جريمة كلاسيكية تمارس في الواقع الافتراضي	3,8000	1,14092	مرتفعة
5	17	تأدي الجريمة الالكترونية الى انتشار الكراهية وفتنة بين الشعوب وبين الشعب الواحد	3,7972	1,00479	مرتفعة
6	16	تأدي الجريمة الالكترونية الى تشويه سمعة الطلبة في مجتمعهم	3,7493	,95475	مرتفعة
7	2	الجريمة الكترونية عمل إرهابي تعاقب عليه القوانين الدولية	3,7465	1,02122	مرتفعة
8	9	يحد قانون العقوبات الجزائري من وقوع الجرائم الالكترونية	3,6000	,80815	متوسطة
9	7	يوجد قانون مستقل للجريمة الإلكترونية في الجزائر	3,5915	1,10440	متوسطة
10	15	ان على دراية بأنواع الجريمة المنتشرة في المواقع الافتراضية	3,5634	1,04331	متوسطة
11	3	الجريمة الإلكترونية هي كل الأضرار التي تلاحق الطلبة والمؤسسة الجامعية من خلال الوسائل الإلكترونية.	3,5268	1,00913	متوسطة
12	14	أدرك أهمية تحديد وتقييم المخاطر السيبرانية واتخاذ الإجراءات الوقائية المناسبة للحد منها	3,4000	1,29449	متوسطة
13	11	اعرف التعامل مع كل من يحاول إساءة لي عبر الأنترانت	3,3746	1,08816	متوسطة
14	12	لدي علم بالإجراءات القانونية لتقديم شكوى عند تعرضي لجريمة الكترونية	3,3352	1,08027	متوسطة
15	10	أدرك أهمية الالتزام بالمعايير القانونية عند التوصل الافتراضي	3,2704	1,01964	متوسطة
16	4	تأدي الجريمة الالكترونية عدم القدرة على الوصول إلى الخدمات الإنترنت	3,2394	,90611	متوسطة
17	8	لدي دراية بقانون العقوبات الخاص بالجريمة الالكترونية في الجزائر	3,2000	,99830	متوسطة
18	13	أدرك خطورة الهجمات الالكترونية على بياناتي الشخصية	2,5127	1,37645	متوسطة
الدرجة الكلية للوعي بالجريمة الالكترونية			**3,5551**	**1,09453**	**متوسطة**

يبين الجدول (18) أن درجة الوعي بالجريمة الالكترونية لدى طلبة كلية العلوم الإنسانية و الاجتماعية، من وجهة نظرهم، جاءت متوسطة، بمتوسط حسابي (3,5551)، وانحراف معياري

(1,09453)، وقد تراوحت المتوسطات الحسابية ما بين (4,3718-2,5127) حيث جاءت الفقرة رقم (1) والتي تنص على: " الجريمة الإلكترونية هي نتاج عن الانتشار الواسع للأنترانت ووسائط الإلكترونية " في المرتبة الأولى وبمتوسط حسابي بلغ (4,3718)، بينما جاءت الفقرة رقم (13) والتي تنص على:" أدرك خطورة الهجمات الالكترونية على بياناتي الشخصية" بمتوسط حسابي بلغ (2,5127) ، وبلغ المتوسط الحسابي للمجال ككل (3,5551).

نستنتج من خلال معطيات الجدول، أن الوعي بالجريمة الإلكتروني لطلبة كان متوسطة بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344)، حيث جاءت 7 عبارات بدرجة عالية اول عبارات كانت رقم 1" الجريمة الإلكترونية هي نتاج عن الانتشار الواسع للأنترانت ووسائط الإلكترونية"، حيث ان الطلبة يعتبرون ان انتشار ظاهرة الجريمة في المواقع الافتراضية هو نتيجة أستخدم الأنترنت في حياتنا اليومية، كما يعتبرون حسب عبارة رقم 5 " كل ابتزاز او سرقة بيانات في الواقع الافتراضي يعتبر جريمة الكترونية " كما يدركون اضرار التقنية للجريمة الإلكترونية، حسب عبارة رقم 18 " تسبب الجريمة الالكترونية أضرار بممتلكات الشخصية والمؤسسات الدولة العمومية والخاصة " كمأنهم يفرقون بين الجريمة الكلاسيكية والحديثة فحسب عبارة رقم 6" الجريمة الالكترونية هي كل جريمة كلاسيكية تمارس في الواقع الافتراضي".

أضافة الى هذا، فهم يعتبرون أن الجريمة الإلكترونية من أسباب انتشار الفتن بين الشعوب وصراع، بين الافراد المجتمع الواحد وهذا من خلال عبارات رقم 17 " تأدي الجريمة الالكترونية الى انتشار الكراهية وفتنة بين الشعوب وبين الشعب الواحد " إضافة الى عبارات رقم16" تأدي الجريمة الالكترونية الى تشويه سمعة الطلبة في مجتمعهم" كما يصنف الطلبة الجريمة الإلكترونية، من الأعمال الإرهابية التي أصبحت تهدد المجتمعات من خلال عبارة رقم7 " الجريمة الكترونية عمل إرهابي تعاقب عليه القوانين الدولية".

كمأننا نلاحظ أن عديد من العبارات التي كانت بدرجة متوسطة، والتي تعكس مستوي وعي الطلبة حول الجريمة الإلكترونية ويستوجب علينا تحليلها وتركيز عليها من خلال بناء البرامج التي تنمي وعي الطلبة

حول هذه الظاهرة، حيث كان ادراكهم متوسط فيما يخص بقانون العقوبات الجزائري في حد من ظاهرة الجريمة الالكترونية، وهذا نتيجة لبعد تخصص عن القانون إضافة الى عدم وعيهم القانوني بالظاهرة كم جاءت معرفتهم متوسطة فيما يخص بمعرفة قانون الجريمة الإلكترونية في التشريع الجزائري،

أما بنسبة، للأنواع الجريمة ليس لديهم معرفة بكل الأنواع التي قد تواجههم خلال استخدام الأنترانت مما يزيد من نسبة وقعهم ضحية لها خاصة من جرائم البريد الإلكترونية على سبيل المثال، ومن أببا هذا يعود هذا "لعدم درايتهم بقانون العقوبات الخاص بالجريمة الالكترونية في الجزائر" حسب عبارة رقم 8 إضافة لعدم " أدركهم خطورة الهجمات الالكترونية على بياناتي الشخصية ".

ومن خلال هذا، يستوجب تنمية وعي الطلبة في الجانب القانوني وأدراك للمخاطر الجريمة الإلكترونية حيث أن كان مستواهم، متوسط في جابة عن العبارة خاصة بهذا الجانب على عكس الوعي المعرفي حول الظاهرة فقد كان مستوي الطلبة مرتفع، ومن خلال مقارنة مع نتائج دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) التي كانت حول الجرائم الإلكترونية ومستوى الوعي بخطورتها عينة من الشباب الجامعي الأردني نجد أن وعيهم بالجريمة الإلكترونية كان مرتفع على عكس نتائج المتوصل عليها

5.2 **عرض وتحليل الجداول المتعلقة بالسؤال الرابع:** هل توجد فروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لكل من متغيرات الجنس، السن، القسم، المستوي التعليمي؟ تم الإجابة عن هذا السؤال عن النحو الاتي:

1.5.2. الجنس

تم حساب المتوسطات الحسابية والانحرافات المعيارية، للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس كما تم تطبيق **اختبار"ت"(t-test)** ويظهر الجدول رقم (29) ذلك.

الجدول (29): المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير الجنس.

البيانات الجنس	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة
ذكر	153	3,1465	,57726	-,022	353	,982	0,05
انثى	202	3,1479	,62711				

يتضح من الجدول رقم (29) قيمة (T) بلغت 022,-وان قيمة الدلالة المحسوبة هي 982, وهي أكبر من قيمة الدلالة المعتمدة 0.05 ،وبالتالي فهي غير دالة إحصائية وهذه النتيجة تدل الى، عدم وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني وفق متغير الجنس ومنه نستطيع القول بأنه تم قبول فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي)" ورفض الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول، أنه لا يوجد فروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي) ، وهي نفس النتيجة التي توصلت اليها كل من دراسة حمد بن حمود السواط وآخرون (2020) ، حيث لم تكن هناك فروق تعزى لمتغير الجنس في مستوي وعي بالأمن السيبراني، لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف ودراسة عبد الله بن حجاب القحطاني (2022) ،بنسبة ذوي الإعاقة البصرية في المملكة العربية السعودية وهذا فاعتماد على برنامج تعليمي موحد بين جنسين لا يأدي الى وجود فروق.

2.5.2. السن

تم حساب المتوسطات الحسابية والانحرافات المعيارية، للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن ويظهر الجدول رقم (30) ذلك.

الجدول (30): المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر تعزى لمتغير السن.

السن	عدد الأفراد (N)	المتوسط الحسابي	الانحراف المعياري
من 17 سنة الى 21 سنة	107	3,0781	,66003
من 22 سنة الى 26 سنة	158	3,1217	,56823
من 27 فما فوق	90	3,2745	,58784
مجموع	355	3,1473	,60529

يلاحظ من الجدول رقم (30) وجود فروق ظاهرية بين المتوسطات الحسابية لمستوى مستوي الوعي السيبراني، لطلبة كلية العلوم الإنسانية والاجتماعية لجامعة جيلالي بونعامة خميس مليانة من وجهة نظرهم، تبعًا لمتغير السن، إذ حصل أصحاب فئة " من 27 فما فوق " على أعلى متوسط حسابي بلغ 3,2745، وجاء أصحاب فئة " من 22 سنة الى 26 سنة " بالرتبة الثانية بمتوسط حسابي بلغ 3,1217، وجاء المتوسط الحسابي لفئة " من 17 سنة الى 21 سنة سنوات" إذ بلغ 3,0781، ولتحديد ما إذا كانت الفروق بين المتوسطات ذات دلالة إحصائية تم تطبيق تحليل التباين الأحادي (One way ANOVA) وجاءت نتائج تحليل التباين على النحو الذي يوضحه الجدول رقم(31).

الجدول (31): تحليل التباين الأحادي (One way ANOVA)، لإيجاد دلالة الفروق للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن.

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية	مستوي الدلالة المعتمدة
بين المجموعات	2,073	2	1,036	2,858	,059	0,05
داخل المجموعات	127,626	352	,363			
المجموع	129,698	354				

يتضح من خلال الجدول رقم (31) قيمة (ف) بلغت 2,858 وان قيمة دلالتها الإحصائية 059, هي أكبر من مستوي الدلالة المعتمدة 0.05 وهذه النتيجة تدل الى عدم وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة، في مستوي الوعي السيبراني وفق متغير السن ومنه نستطيع القول بأنه تم قبول فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية

والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن (من 17 سنة الى 21سنة ، من 22 سنة الى 26سنة، من 27 فما فوق)" ورفض الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن (من 17 سنة الى 21سنة ، من 22 سنة الى 26سنة، من 27 فما فوق)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول أنه لا يوجد فروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن، وهي عكس النتيجة التي توصلت اليها ايمان عبد الفتاح عبابنه (2022) قيما يخص الخبرة التدريسية حيث استنتجت فروق ذات دلة إحصائية بنسبة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني، ومن خلال هذا يمكن يعتبر أن للتعليم والتدريب دور في تمكين الطالب في زيادة وعيه السيبراني فسن الطالبة ليس مؤثر في الوعي دون تدريب و تعلم.

3.5.2. القسم

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي السيبراني، للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم كما تم تطبيق اختبار"ت"**(t-test)** ويظهر الجدول رقم (32) ذلك.

الجدول رقم (32): المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير القسم.

البيانات القسم	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة
العلوم الاجتماعية	173	3,0435	,63506	-3,180	353	,002	0,05
العلوم الإنسانية	182	3,2460	,55967				

يتضح من الجدول رقم (32) قيمة (T) بلغت 3,180-وان قيمة الدلالة المحسوبة هي 002, وهي أصغر من قيمة الدلالة المعتمدة 0.05، وبالتالي فهي دالة إحصائية وهذه النتيجة تدل الى وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني وفق متغير القسم للصالح قسم العلوم الإنسانية، بمتوسط حسابي (3,2460) وانحراف معياري (55967,) ، ومنه نستطيع القول بأنه تم رفض فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم (العلوم الاجتماعية ، العلوم الإنسانية)" وقبول الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم (العلوم الاجتماعية ، العلوم الإنسانية)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول أنه يوجد فروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم وهذا راجع للآن تخصصات العلوم الإنسانية، مثل علوم الأعلام والاتصال تهتم بتقنيات والوسائط التكنلوجية لهذا نجد طلبتها أوعي من طلبة علوم الاجتماعية.

4.5.2. المستوي التعليمي

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي السيبراني، للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى، لمتغير المستوي التعليمي، كما تم تطبيق **اختبار"ت"(t-test)** ويظهر الجدول رقم (33) ذلك.

الجدول رقم (33): المتوسطات الحسابية والانحر افات المعيارية للمستوي الوعي السيبر اني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير المستوي التعليمي.

البيانات	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة

المستوي التعليمي							
لسانس	243	3,1757	,60502	1,305	353	,193	0.05
ماستر	112	3,0856	,60397				

يتضح من الجدول رقم (33) قيمة (T) بلغت 1,305وان قيمة الدلالة المحسوبة هي 193,وهي أكبر من قيمة الدلالة المعتمدة 0.05 وبالتالي فهي غير دالة إحصائية وهذه النتيجة تدل الى، عدم وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني وفق متغير المستوي التعليمي، ومنه نستطيع القول بأنه تم قبول فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي (لسانس، ماستر)" ورفض الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية، لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي (لسانس، ماستر)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول أنه، لا يوجد فروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي، وهي عكس النتيجة التي توصلت اليها ايمان عبد الفتاح عبابنه (2022) ،فيما يخص المؤهل العلمي حيث استنتجت فروق ذات دلة إحصائية بنسبة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني، ومن خلال هذا يمكن يعتبر أن محتوي المقررات التعليمة، في الأطوار الثلاثة في وزارة التعليم والتربية و مقايس العلوم الاجتماعية و الإنسانية التركيز على الجانب تنمية مهارات الطلبة في الجان التكنلوجي والأمني للتنمية وعيه السيبراني.

6.2 عرض وتحليل الجداول المتعلقة بالسؤال الخامس: هل توجد فروق في مستوي وعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لكل من متغيرات الجنس، السن، القسم، المستوي التعليمي؟ تم الإجابة عن هذا السؤال عن النحو الاتي:

1.6.2.الجنس

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس، كما تم تطبيق **اختبار"ت"(t-test)** ويظهر الجدول رقم (34) ذلك.

الجدول رقم (34): المتوسطات الحسابية والانحرافات المعيارية للمستوي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير الجنس.

البيانات الجنس	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة
ذكر	153	3,4818	,53241	-2,323	353	,021	0,05
انثى	202	3,6177	,55563				

يتضح من الجدول رقم (34) قيمة (T) بلغت 2,323-وان قيمة الدلالة المحسوبة هي 021, وهي أصغر من قيمة الدلالة المعتمدة 0.05، وبالتالي فهي دالة إحصائية وهذه النتيجة تدل الى وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة، في مستوي الوعي بالجريمة الإلكترونية وفق متغير الجنس للصالح الإناث بمتوسط حسابي (3,6177) وانحراف معياري (55563,) ومنه نستطيع القول بأنه تم رفض فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي)" وقبول الفرضية البديلة القائلة بـ: "توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية

العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول، أنه يوجد فروق في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير الجنس (ذكر، أنثي) على عكس النتائج المتوصل اليها في دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) حول الجرائم الإلكترونية، ومستوى الوعي بخطورتها: على عينة من الشباب الجامعي الأردني حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير الجنس لدي الشباب الجامعي الأردني، بحكم معرفتهم بحقوقهم وواجبتهم عند استخدام الأجهزة الإلكترونية، على عكس الطلبة الجزائري حيث ذهبت الفروق لصالح الإناث بحكم توجيه التوعية بمخاطر الجريمة الإلكترونية خصيصا لها من قبل الأسرة كونها الأكثر استهدافا.

2.6.2.السن

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن، ويظهر الجدول رقم (35) ذلك.

الجدول (35): المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر تعزى لمتغير السن.

السن	عدد الأفراد (N)	المتوسط الحسابي	الانحراف المعياري
من 17 سنة الى 21 سنة	107	3,5130	,57500
من 22 سنة الى 26 سنة	158	3,5334	,53294
من 27 فما فوق	90	3,6593	,53916
مجموع	355	3,5592	,54913

يلاحظ من الجدول رقم (35) وجود فروق ظاهرية بين المتوسطات الحسابية لمستوى مستوي الوعي بالجريمة الإلكترونية لطلبة كلية العلوم الإنسانية والاجتماعية لجامعة جيلالي بونعامة خميس مليانة من وجهة نظرهم، تبعًا لمتغير السن، إذ حصل أصحاب فئة " من 27 فما فوق " على أعلى متوسط حسابي بلغ

3,6593، وجاء أصحاب فئة " من 22 سنة الى 26 سنة" بالرتبة الثانية بمتوسط حسابي بلغ 3,5334، وجاء المتوسط الحسابي لفئة " من 17 سنة الى 21 سنة سنوات" إذ بلغ 3,5130، ولتحديد ما إذا كانت الفروق بين المتوسطات ذات دلالة إحصائية تم تطبيق تحليل التباين الأحادي (One way ANOVA)، وجاءت نتائج تحليل التباين على النحو الذي يوضحه الجدول رقم(37).

الجدول (36): المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر تعزى لمتغير السن.

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية	الدلالة المعتمدة
بين المجموعات	1,235	2	,617	2,060	,129	0,05
داخل المجموعات	105,511	352	,300			
المجموع	106,745	354				

يتضح من خلال الجدول رقم (36) قيمة (ف) بلغت 2,060وان قيمة دلالتها الإحصائية 129, هي أكبر من مستوي الدلالة المعتمدة 0.05 وهذه النتيجة تدل الى عدم وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي بالجريمة الإلكترونية، وفق متغير السن ومنه نستطيع القول بأنه تم قبول فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن (من 17 سنة الى 21سنة ، من 22 سنة الى 26سنة، من 27 فما فوق)" ورفض الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن (من 17 سنة الى 21سنة ، من 22 سنة الى 26سنة، من 27 فما فوق)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول، أنه لا يوجد فروق في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير السن على عكس النتائج، المتوصل اليها في دراسة أنوبريت كور موخا (2017) التي حول وعي بجرائم الإنترنت والأمان

في منطقة دلهي، وهذا يعكس مستوي استخدام الأنترانت حيث تعتبر هذا نوع من جريمة جديد على مجتمعنا عكس مجتمعات الدول المتقدمة، حيث أصبحت الجريمة الإلكترونية أكثر ملاحظة لدي جميع الفئات العمرية عكس مجتمع الجزائري.

3.6.2.القسم

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم، كما تم تطبيق **اختبار"ت"(t-test)** ويظهر الجدول رقم (37) ذلك.

الجدول رقم (37): المتوسطات الحسابية والانحرافات المعيارية للمستوي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير القسم.

البيانات القسم	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة
العلوم الاجتماعية	173	3,4900	,57684	-2,320	353	,021	0,05
العلوم الإنسانية	182	3,6248	,51444				

يتضح من الجدول رقم (37) قيمة (T) بلغت 2,320-وان قيمة الدلالة المحسوبة هي021, وهي أصغر من قيمة الدلالة المعتمدة 0.05 وبالتالي فهي دالة إحصائية وهذه النتيجة تدل الى وجود فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي بالجريمة الإلكترونية وفق متغير القسم للصالح العلوم الإنسانية بمتوسط حسابي (3,6248) وانحراف معياري (51444,) ومنه نستطيع القول بأنه تم رفض فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية، للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم (العلوم الاجتماعية ، العلوم الإنسانية)" وقبول الفرضية البديلة القائلة بـ: "توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من

وجهة نظر الطلبة تعزى لمتغير القسم (العلوم الاجتماعية ، العلوم الإنسانية)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول، أنه يوجد فروق في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير القسم على عكس النتائج، المتوصل اليها في دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) حول الجرائم الإلكترونية ومستوى الوعي بخطورتها: على عينة من الشباب الجامعي الأردني حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير التخصص لدي الشباب الجامعي الأردني بحكم درجة المعرفة بالظاهرة مرتفعة إضافة الى أن عينة الدارسة من الطلبة علم اجتماع الانحراف و الجريمة، وبهذا نستنتج أن لتخصص العلمي دور في ادراك الطلبة للجريمة الإلكترونية وهذا مفسر الفروق بين طلبة قسم العلوم الإنسانية والاجتماعية، ودور مقايس التي تهتم بالأعلام و الاتصال و الوسائط الإلكترونية في تنمية الوعي بظاهرة.

4.6.2.المستوي التعليمي

تم حساب المتوسطات الحسابية والانحرافات المعيارية للمستوي الوعي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي، كما تم تطبيق اختبار"ت"(t-test) ويظهر الجدول رقم (38) ذلك.

الجدول (38): المتوسطات الحسابية والانحر افات المعيارية للمستوي بالجريمة الالكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة واختبار"ت" (t-test) تعزى لمتغير المستوي التعليمي.

البيانات المستوي التعليمي	عدد الأفراد N	المتوسط الحسابي	الانحراف المعياري	قيمة (T)	درجة الحرية	الدلالة المحسوبة	الدلالة المعتمدة
لسانس	243	3,5768	,53415	,892	353	,373	0,05
ماستر	112	3,5208	,58091				

يتضح من الجدول رقم (38) قيمة (T) بلغت 892, وان قيمة الدلالة المحسوبة هي373, وهي أكبر من قيمة الدلالة المعتمدة 0.05 وبالتالي فهي غير دالة إحصائية وهذه النتيجة تدل الى عدم وجود فروق ذات

دلالة إحصائية، بين افراد عينة الدراسة في مستوي الوعي بالجريمة الإلكترونية وفق متغير المستوي التعليمي، ومنه نستطيع القول بأنه تم قبول فرضية القائلة " لا توجد فروق ذات دلالة احصائية في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي (لسانس، ماستر)" ورفض الفرضية البديلة القائلة بـ: " توجد فروق ذات دلالة احصائية في الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي (لسانس، ماستر)" ونسبة التأكد من هذه النتيجة المتوصل إليها هي 95% مع احتمال الوقوع في الخطأ بنسبة 5%.

ونستنتج من خلال معطيات الجدول أنه لا يوجد فروق في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة تعزى لمتغير المستوي التعليمي وقد توافقت دراستنا مع النتائج المتوصل اليها في دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) حول الجرائم الإلكترونية ومستوى الوعي بخطورتها: على عينة من الشباب الجامعي الأردني حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير المستوي لدي الشباب الجامعي الأردني، وبهذا نستنتج أن المعرفة و أدراك الجريمة الإلكترونية لا تقتصر علي مستوي التعليمي للفرد فهي مثلها مثل الجريمة الكلاسيكية تفرض على الفرد أدراك خطورتها لتجنب الوقع ضحية لها.

7.2 عرض وتحليل الجداول المتعلقة بالسؤال السادس: هل توجد علاقة ارتباطية بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة؟

للإجابة عن هذا السؤال تم حساب معامل الارتباط باستخدام معامل الارتباط بيرسون، بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة ويظهر الجدول رقم (39) ذلك.

الجدول (39): معامل الارتباط بين بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة، باستخدام معامل الارتباط بيرسون.

//////		الوعي بالجريمة الإلكترونية
الوعي السيبراني	معامل الارتباط	,594**
	مستوى الدلالة	,000
	حجم العينة	355
الارتباط دال عند (α=0,01).		

يتضح من الجدول رقم (39) أن معامل الارتباط بيرسون بلغ معامل الارتباط (**0,594**) بين الوعي السيبراني والوعي بالجريمة الإلكترونية وهي قيمة موجبة ومرتفعة، وهذا يعني أن الارتباط بينهما ارتباط طردي، أي أنه كلما ارتفعت درجات الوعي السيبراني ارتفعت معها الوعي بالجريمة الإلكترونية والعكس صحيح، كما أن نتيجة هذا الارتباط جاءت دالة إحصائيا بمستوى دلالة 000,، أي أنها دالة إحصائية عند مستوى $\alpha \leq 0.05$ ومنه نستطيع القول بأنه تم رفض فرضية القائلة "لا توجد علاقة ارتباطية بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة" وقبول الفرضية البديلة القائلة بـ: " توجد علاقة ارتباطية بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة".

نستنتج من خلال معطيات الجدول، وجود علاقة ارتباطية بين الوعي السيبراني والوعي بالجريمة فكلما كان مستوي الوعي السيبراني عالي، يأثر على مستوي أدراك الطالب للجريمة الإلكترونية فالوعي السيبراني يربط بمجال الأمن السيبراني، فكلما كان لطالب معرفة بأساسياتهم في جانب المهارات و أتخذ السلوك الأمني مناسب، في حالة تعرض للهجمة الكترونية عند استخدام الأنترانت أدي ذالك الى تجنب وقوع ضحية لنوع من أنوع الجريمة السيبرانية، و هذا ما تعكسه نتائج الدرجة الكلية لكل من الوعي السيبراني، والوعي بالجريمة الإلكترونية التي كانتا متوسطة وبهذا واجب على جميع الطلبة عند استخدم الإنترنت، أن

يكونوا على دراية بجرائم الإنترنت والأمان الأنترانت، من خلال زيادة الوعي بينهم و تطوير مهارتهم في الاستخدام الأمن للوسائط الإلكترونية لتحقيق شعور بالأمن.

8.2 تحليل ومناقشة النتائج الجزئية

1.8.2. عرض النتائج الجزئية المتعلقة: بالوعي السيبر اني والجريمة الإلكترونية من وجهة نظر طلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة

بعد عرض تحليل وتفسير، المعطيات المحصل عليها ميدانيا وذلك في شكل جداول وأشكال توضيحية استنتجنا من خلال وجهة نظر الطلبة ان لكل من الوعي السيبراني والجريمة الإلكترونية أساسية في العملية البحثة واكتشاف ما يعرفه العينة الأساسية، حول الظاهرة الجريمة الإلكترونية والوعي السيبراني باعتبارها نتاج عن التطور التكنلوجي الذي وصلت اليه البشرية وارتباطها بالأنترنت، حيث كانت نسبة 53.23% من الطلبة يستخدمون الأنترانت دائما مقابل، 28.17% من نسبة الطلبة يستخدمون الأنترانت أحيانا حيث يقضي نسبة 61.97% من الطلبة يستخدمون الأنترانت أكثر من 3ساعات وهي نسبة عالية تعبرعن ادمان الطلبة للاستخدام لها.

حيث تنوعت أسباب استخدام الطلبة للأنترانت فنسبة 35.49% من الطلبة يستخدمون الأنترانت للتعلم، مقابل نسبة 27.90% الطلبة يستخدمون الأنترانت للدردشة، وتكوين صدقات اما بقي الطلبة كانت استخداماتهم لها في العمل، عن بعد ومشاهدة الأفلام والبرامج.

فاستخدام الأنترانت يفرض على الطالب أدراك أساسية الاستخدام حيث كان أغلب الطلبة معرفتهم بمجال الأمن السيبراني، بين متوسطة ومنخفضة فقد بلغت أن نسبة 59.15%من الطلبة مستوي معرفتهم بالأمن السيبراني، متوسطة مقابل نسبة 22.55% مستوي معرفتهم بالأمن السيبراني منخفضة وكان الوعي السيبراني في نظرهم تنفيذ الأنشطة عبر الإنترنت بشكل آمن ب نسبة47.90%، مقابل نسبة 29.57% في نظرهم الوعي السيبراني هو الوعي بالمخاطر الهجمات الإلكترونية.

ومن بين الأنشطة التي يجنبها الطلبة على الإنترنت للحافظ على أمانهم هي عدم الدخول إلى مواقع غير آمنة، بنسبة 45.07% لتجنب سرقة بياناتهم وتعرض أجهزتهم الى الفيروسات ومن بين الخطوات الأساسية التي يتبعها الطلبة لتعزيز امنهم السيبراني، 40.84% منهم يقمون بتحديث البرامج الخاص بجهازي (حاسوب/الهاتف) ، مقابل 25.35% من نسبة الطلبة يستخدمون كلمات مرور قوية ومتنوعة بصفة دورية، بنسبة لكل من (البريد الإلكتروني/مواقع التواصل الاجتماعي) ، كمأنهم يعتبرون أن للوعي السيبراني أهمية في واقع الافتراضي حيث أن 46,47% من يعتبرونه أساسي في الوقاية من الهجمات والجرائم الإلكترونية مقابل 29,59% هي زيادة أمانهم عند استخدام الإنترنت.

أما بنسبة للجريمة الإلكترونية، كانت معرفة الطلبة لها متوسطة بنسبة قدرت أن47,00%من الطلبة مستوي معرفتهم بالجريمة الالكترونية، وهذا بحكم أن ظاهرة حديثة بنسبة للمجتمع الجزائري، وبحكم أنهم مستخدمو للأنترانت و مواقع التواصل الاجتماعي كإنو يلاحظون العديد من الظواهر الإجرامية في الحياة الافتراضية، وأبرزها هي القذف والسب مثل (ترويج أخبار الكاذبة/تقليل من الاحترام/مساس بكرامة) و الجرائم غير الأخلاقية مثل (مواقع غير الأخلاقية/صور جنسية) بمجموع نسبي قدر 50% من مجموع العام لطلبة وكثير من الطلبة وقع ضحية لها وتعرض 48,45% من الطلبة ضحايا لها مرة واحدة، مقابل 33,25% من الطلبة الذين وقع ضحايا لها من جريمتين الى ثلاث جرائم، ومن بين الجرائم كانت الشتم والتهديد بنسبة 27,00%، و 25,00% من الطلبة تعرضوا للقرصنة حسابتهم خاص بالتوصل الاجتماعي.

كمأن 80,29% من الطلبة لم يرفعوا شكوى عند الشرطة لعدم معرفتهم بقانون الجريمة الإلكترونية فغياب لمعرفة بقوانين التشريعية الجزائرية للجريمة الإلكترونية، هي أحد عوامل وقع ضحية للجريمة الإلكترونية، ومن حلول لتنمية الوعي السيبراني للجريمة الالكترونية في الوسط الجامعي في نظر الطلبة هي، تشجيع الإبلاغ عن الحوادث السيبرانية مع الطلبة توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني.

2.8.2. عرض النتائج الجزئية المتعلقة: بالوعي السيبراني لطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة

يعتبر الوعي السيبراني هو معرفة أساسيات بمهارات الاستخدام الأمن للوسائط الإلكترونية وكان الهدف الأساسي، هو معرفة درجة مستوي الطلبة وتقيمه وتركيز على العناصر التي يدركونها ونقاط ضعفهم التي يستوجب أستدركها حيث أن درجة الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية، من وجهة نظرهم جاءت متوسطة، بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344) وقد تراوحت المتوسطات الحسابية ما بين (3,9859-2,3239) حيث انهم يركزون في حفاظ على أمنهم السيبراني، من خلال عدم مشاركة بيناتهم مع الغرباء، وهذا يعتبر سلوك للحيطة فقط للأن تقنيات الاختراق أصبحت أكثر تطورا مم يساهم في سرقة بيناتهم عن طريق الثغرات الإلكترونية، في نظام المعلوماتي للأجهزتهم حيث يخشي الطلبة انتهاكات الامن السيبراني، بمتوسط حسابي (3,7211)، وانحراف معياري (1,13917) ويعتبرون الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة بمتوسط حسابي (3,8479)، وانحراف معياري (,97393).

ومن بين نقاط التي نستنتجها من خلال تقيم لدرجة الوعي السيبراني، فقد كان الجانب المعرفي للوعي السيبراني أعلى درجة حيث كل الطلبة يعتبرون أن الوعي السيبراني يخص الاستخدام الأنترانت، وموقع التواصل الاجتماعي أما هنالك من جونب التي كانت درجة وعيهم متوسطة، والتي يستوجب التركيز عليها في تنميتها ومنها هي عدم اطلاعهم على الجرائم والهجمات السيبرانية، وعدم قراءة اتفاقيات المستخدم لبرنامج مجاني قبل موافقة و عدم التقيد بالسلوكيات الواعية، في توفير جوى أمن خلال استخدام الأنترانت مما يزيد فرص وقعهم ضحيا للهجمات السيبرانية.

وفي أطار معرفة أراءهم حول سبل تعزيز وتنمية الوعي السيبراني فيعتبرون ان تبادل الطلبة معلومات حول التهديدات السيبرانية، يساهم في تنمية أصافة الى الحملات التوعوية وتطلع على الأخبار كمأنهم كانو مهتمين بتحقيق وقاية والأمن السيبراني، وليس لديهم أي معوقات تمنعهم.

ومن خلال مقارنة درجة الكلية وعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة مع نتائج الدارسات السابقة، التي كانت لها نفس موضوعنا البحثي استنتجنا مع درجة الوعي بالأمن السيبراني لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، حيث توصلت دراسة الباحث حمد بن حمود السواط وآخرون (2020) لدي تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف درجة عالية في وعيهم بمجال حماية الأجهزة الإلكترونية، ومجال التعامل مع أمن المتصفح بالإضافة الى درجة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن، فقد توصلت الباحثة ايمان عبد الفتاح عبابنه (2022) الى أن معلمات كانت درجة وعيهم عالية جدا، أما الباحث عبد الله بن حجاب القحطاني (2022) فقد توصلت دراسته ان درجة الوعي بالأمن السيبراني لدى ذوي الإعاقة البصرية في المملكة العربية السعودية كانت درجة وعيهم بمفاهيم الوعي الأمن السيبراني متوسطة، ومرتفعة بنسبة الوعي بتطبيقات الأمن السيبراني وسبل تعزيز الأمن السيبراني، على عكس طلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة التي كانت متوسطة، وهذا يرجع الى اختلاف أولا المقررات التعليمة معتمدة في بلدانهم، والتي تهتم بتوعية وتطوير المهارات الأمن السيبراني.

ام بنسبة للفروق في مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة، فلم تكن فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني وفق متغير (الجنس، السن، والمستوي التعليم) وقد كانت الفروق وفق متغير القسم، للصالح قسم العلوم الإنسانية بمتوسط حسابي (3,2460) وانحراف معياري (55967,)

ومن خلال مقارنتها مع نتائج الدارسات السابقة التي درست نفس متغيرات الديمغرافية لدراستنا نستنتج، أنه من حيث متغير الجنس كانت نفس النتيجة التي توصلت اليها كل من دراسة الباحث حمد بن حمود السواط وآخرون (2020)، والباحث بن حجاب القحطاني (2022) لم تكن هناك فروق تعزى لمتغير الجنس في مستوي وعي بالأمن السيبراني لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف وذوي الإعاقة البصرية في المملكة العربية السعودية.

أم بنسبة لمتغير السن كانت هنالك اختلاف مع دراسة الباحثة ايمان عبد الفتاح عبابنه (2022) فيما يخص الخبرة التدريسية، حيث استنتجت فروق ذات دله إحصائية بنسبة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني.

أما بنسبة لمتغير المستوي التعليمي، فقد توصلت الباحثة ايمان عبد الفتاح عبابنه (2022)، قيما يخص المؤهل العلمي حيث استنتجت فروق ذات دله إحصائية بنسبة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني.

3.8.2. عرض النتائج الجزئية المتعلقة: بالوعي بالجريمة الإلكترونية طلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة

باعتبار الجريمة الإلكترونية هي نتيجة لنشاطات السيبرانية للفرد من خلال مواقع الويب والشبكات الاجتماعية وتطبيقات الدردشة والمدونات والألعاب عبر الإنترنت والمراسلين والبريد الإلكتروني وتعد مشكلة أخلاقية، تتجمع فيها العديد الأسباب التي يمكن للطالب الجامعي ضحية لها والوعي بها وبمخاطرها وبأشكالها مثل التمييز، الإساءة، والترهيب، والتهميش، وأخرى، تغيب فيها صفات الإنسانية، وتبرز جانب الغير الأخلاقي وتعتبر من الأسباب لقياس مستوي وعيهم بالجريمة الإلكترونية، كظاهرة حيث كانت درجة الوعي بالجريمة الالكترونية لدى طلبة كلية العلوم الإنسانية و الاجتماعية من وجهة نظرهم، جاءت متوسطة بمتوسط حسابي (3,5551)، وانحراف معياري (1,09453).

حيث كان الطلبة يدركون بدرجة عالية أن الجريمة الإلكترونية، هي نتاج عن الانتشار الواسع للأنترانت، ووسائط الإلكترونية بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344)،

فهم يعتبرون ان انتشار ظاهرة الجريمة في المواقع الافتراضية، هو نتيجة أستخدم الأنترنت في حياتنا اليومية كما يدركون مخاطر الناتجة عنها وأضرارها على ممتلكات الشخصية، والمؤسسات الدولة العمومية والخاصة.

ومن الجوانب التي أثرت على درجة وعيهم بالجريمة الإلكترونية ويستوجب علينا تحليلها وتركيز عليها من خلال، بناء البرامج التي تنمية وعي الطلبة حول هذه الظاهرة هي جانب القانوني مثل قانون الجريمة الإلكترونية في التشريع الجزائري، حيث كانت درجة وعيهم له متوسطة وهذا ما يساهم في بوقوع الطلبة جنات او ضحايا، لهذه الجريمة ومن خلال مقارنة مع نتائج دراسة غدير برنس وعبد الكريم عوده الله الخرابشة (2020) التي كانت حول الجرائم الإلكترونية ومستوى الوعي بخطورتها عينة من الشباب الجامعي الأردني نجد أن وعيهم بالجريمة الإلكترونية كان مرتفع على عكس نتائج المتوصل عليها.

ام بنسبة للفروق في مستوي الوعي بالجريمة الإلكترونية للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة من وجهة نظر الطلبة، فلم تكن فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني، وفق متغير (السن، والمستوي التعليم) وقد كانت الفروق ذات دلالة إحصائية، وفق متغير الجنس للصالح الإناث بمتوسط حسابي (3,6177) وانحراف معياري (55563,) أضافة الى الفروق ذات دلالة إحصائية وفق متغير القسم للصالح العلوم الإنسانية بمتوسط حسابي (3,6248) وانحراف معياري (51444,).

ومن خلال مقارنتها مع نتائج الدارسات السابقة، التي درست نفس متغيرات الديمغرافية لدراستنا نستنتج أنه من حيث متغير الجنس كانت نتائج دراستنا، على عكس دراسة الباحثين غدير برنس وعبد

الكريم عوده الله الخرابشة (2020)، حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير الجنس لدي الشباب الجامعي الأردني.

اما بنسبة لمتغير السن كانت نتائج دراستنا، على عكس نتائج دراسة الباحث أنوبريت كور موخا (2017) حيث لم توجد فروق ذات دلالة إحصائية، تعزي لمتغير السن عند مستخدمي الأنترانت حول وعي بجرائم الإنترنت والأمان في منطقة دلهي.

اما بنسبة لمتغير القسم، كانت نتائج دراستنا على عكس دراسة الباحثين غدير برنس وعبد الكريم عوده الله الخرابشة (2020) حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير التخصص لدي الشباب الجامعي الأردني، فقد توفقت درستنا مع دراستهم بنسبة لمتغير المستوي التعليمي حيث لم توجد فروق ذات دلالة إحصائية تعزي لمتغير المستوي لدي الشباب الجامعي الأردني وبهذا نستنتج أن المعرفة، و أدراك الجريمة الإلكترونية لا تقتصر علي مستوي التعليمي للفرد فهي مثلها مثل الجريمة الكلاسيكية، تفرض على الفرد أدراك خطورتها لتجنب الوقع ضحية لها.

9.2 الاستنتاج العام للدراسة

إن أهم ما نستنتجه من الدراسة الميدانية والتي تناولت مستوي الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية، كانت دراسة ميدانية على عينة من طلبة كلية العلوم الإنسانية والاجتماعية بجامعة جيلالي بونعامة مدينة خميس مليانة ولاية عين الدفلى حيث تندرج في حقل العلوم الاجتماعية تخصص علم الاجتماع الجريمة والانحراف.

حيث تعتبر الجريمة من المشكلات التي يهتم بها هذا التخصص العلمي لكن من الجوانب التي كان يركز عليها الباحثين من قبل هي الدارسات الاستكشافية، واعتماد على المنهج الكيفي للوصل الي الحقيقة العلمية لكن من خلال درستنا، قد كان هدف هو دراسة موضوع الجريمة الإلكترونية من جانب أدراكي، من خلال اعتماد على منهج الكمي وفرضيات الإحصائية للوصل الى هدف الأساسي لدراسة وهو أجاد العلاقة

بين الوعي السيبراني و الوعي بالجريمة الإلكترونية بحكم اختلاف المفهومين، من جانب الخصاص المكونة لهم فالجريمة الإلكترونية هي ظاهرة افتراضية طورتها العولمة من خلال نقلها من الواقع المادي الى، الواقع الافتراضي اما الوعي السيبراني هو الجانب من السلوك الأمني الذي يستوجب أن يكون لدي الطالب.

فقد استنتجنا وجود علاقة ارتباطية موجبة بين الوعي السيبراني، والوعي بالجريمة الإلكترونية بمعامل ارتباط قدر ب (**594,) ومستوي دالة (000,) ،أي أنها دالة إحصائية عند مستوى $\alpha \leq 0.05$ حيث تم قبول الفرضية البديلة القائلة بـ: " توجد علاقة ارتباطية بين مستوي الوعي السيبراني للطلبة كلية العلوم الإنسانية والاجتماعية لجامعة خميس مليانة ووعيهم بالجريمة الإلكترونية من وجهة نظر الطلبة" كمأن كلما كان مستوي الوعي السيبراني لطالب عالي كانت درجة الوعي بالجريمة الإلكترونية عالية، و هذا ما يساهم في تقليل من وقع ضحية للجريمة الإلكترونية.

كمأننا استنتجنا من خلال محور الوعي السيبراني والجريمة الإلكترونية من وجهة نظر طلبة أن نسبة 53.23% من الطلبة يستخدمون الأنترانت دائما وتعددت أسباب الاستخدام للأنترانت فنسبة 35.49%،من الطلبة يستخدمون الأنترانت للتعلم مقابل نسبة 27.90% الطلبة يستخدمون الأنترانت للدردشة وتكوين صدقات اما بقي الطلبة كانت استخداماتهم لها في العمل عن بعد ومشاهدة الأفلام والبرامج كمأنا نسبة 59.15%، من الطلبة مستوي معرفتهم بالأمن السيبراني متوسطة مقابل نسبة 22.55%، مستوي معرفتهم بالأمن السيبراني منخفضة أما بنسبة للجريمة الإلكترونية كانت معرفة الطلبة لها متوسطة، بنسبة قدرت أن47,00%من الطلبة مستوي معرفتهم بالجريمة الالكترونية حيث ان 80,29%، من الطلبة لم رفعوا شكوى عند الشرطة لعدم معرفتهم بقانون الجريمة الإلكترونية، حيث كان 48,45% من الطلبة وقع ضحايا لها مرة واحدة مقابل 33,25% من الطلبة الذين وقع ضحايا للجريمة الالكترونية من جريمتين الى ثلاث جرائم ومن بين الجرائم كانت الشتم والتهديد بنسبة 27,00%، و من حلول لتنمية الوعي السيبراني للجريمة

الالكترونية في الوسط الجامعي في نظر الطلبة هي تشجيع الإبلاغ عن الحوادث السيبرانية مع الطلبة توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني.

كمأننا استنتجنا أن درجة الوعي السيبراني لدى طلبة كلية العلوم الإنسانية والاجتماعية من وجهة نظرهم جاءت متوسطة، بمتوسط حسابي (3,1609)، وانحراف معياري (1,15344)، وقد تراوحت المتوسطات الحسابية ما بين (3,9859-2,3239).

أما بنسبة لفروق فلم تكن فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي الوعي السيبراني وفق متغير (الجنس، السن، والمستوي التعليم) وقد كانت الفروق وفق متغير القسم للصالح قسم العلوم الإنسانية بمتوسط حسابي (3,2460) وانحراف معياري (55967,).

كمأننا استنتجنا أن درجة الوعي بالجريمة الالكترونية لدى طلبة كلية العلوم الإنسانية والاجتماعية، من وجهة نظرهم، جاءت متوسطة، بمتوسط حسابي (3,5551)، وانحراف معياري (1,09453).

أما بنسبة لفروق، فلم تكن فروق ذات دلالة إحصائية بين افراد عينة الدراسة في مستوي بالجريمة الالكترونية وفق متغير (السن، والمستوي التعليم) وقد كانت الفروق ذات دلالة إحصائية وفق متغير الجنس للصالح الإناث بمتوسط حسابي (3,6177) وانحراف معياري (55563,) أضافة الى الفروق ذات دلالة إحصائية وفق متغير القسم للصالح العلوم الإنسانية بمتوسط حسابي (3,6248) وانحراف معياري (51444,).

ونستخلص في الأخير، أن الجريمة الإلكترونية من المواضيع التي يستوجب التركيز عليها من طرف الباحثين والأخصائيين بحكم مخاطر الاقتصادية، والاجتماعية.....الخ، حتى يتسنى لسلطات الأمنية في الجزائر الحد منها، وتقليل ضحيها حيث من خلال موضوعنا الذي كان حول مستوي الوعي السيبراني في الوسط الجامعي الجزائري، وعلاقته بالجريمة الإلكترونية قد كانت النتائج تبين حاجة لعينة الطلبة باعتبارها من مستخدمي الأنترانت، و من فئة المثقفة في مجتمع الى أنها تعرف مستوي متوسط في تحقيق

الاستخدام الأمن للأنترانت، وبهذا يستوجب تمنية الوعي السيبراني للجريمة الإلكترونية، حتي يكون للمورد البشري دور في الحد لها وليس ضحية أو جاني.

- **خاتمة**

تعد الجامعات من أهم مؤسسات التعليم في المجتمع الجزائري، بحكم أهميتها في تكوين واعداد الكفاءات البشرية المتخصصة في شتى المجالات، و نتيجة للتطورات التي يشهدها العصر الحديثة، خاصة مع انتشار الواسع للأنترانت في الوسط الجامعي واستخدامها الذي يشمل جميع المجالات الإدارية والتعليمة، أصبح من تحديات الاجتماعية عامة، وبشكل خاص للمؤسسات الجامعية الجزائري هو تنمية الوعي السيبراني والوعي بالجريمة الإلكترونية للموردها البشري من طلبة وأساتذة و موظفين الإداريين كون أن الوعي السيبراني، يحسن قدرتهم كونهم من المستخدمين للشبكة الأنترانت والوسائط التكنلوجية، على حماية معلوماتهم الشخصية وخصوصيتها على مواقع التواصل الاجتماعي وبياناتهم الرقمية حيث تمكنهم من التميز بين المعلومات الحقيقة والمصادر الموثوقة، التي تكون في شكل مواقع او أشخاص التي تهدد وتضر، بالنظام المؤسسة الجامعية ومستخدمها ومن بينها الهجمات السيبرانية أما الوعي بالجريمة الإلكترونية هي أدارك للأعمال الغير المشروعة التي يتم استخدام الكمبيوتر فيها كأداة، هدف، أو كليهما، في عديد من صورها مثل الانتحال والسرقة والابتزاز والتهكير يمكن استخدام الكمبيوتر كوسيلة في العديد من الأنشطة الإلكترونية الغير قانونية، مثل التعاملات الوهمية والتلاعب والتغيير في بيانات والتي تشكل مخاطر على المورد البشري للوسط الجامعي ونتيجة لتواجد العلاقة بين الوعي السيبراني، والوعي بالجريمة الألكترونية كظاهرة افتراضية لكن أضرارها تجمع بين العالم المادي، والافتراضي نتيجة التطور التكنلوجي مما سهل انتقال السلوكات الاحترافية بينهما، ومن خلال هذا اصبح تجمع كل الأخصائيين و مسؤولين في الجزائر في تنمية الوعي السيبراني للجريمة الألكترونية من خلال مخططات استراتيجية على المدى القصير والبعيد

لتطوير الوعي الاجتماعية الجزائري وتحقيق الأمن الشامل من خلال الجمع بين تطوير التقني و البنية الرقمية و التطوير البشري من خلال مشاريع البحثية و القوانين الردعية .

- **توصيات**

بناء على النتائج السابقة التي توصلت اليها الدراسة، فان هناك مجموعة من التوصيات التي يأمل الباحث أن يؤخذ بها من أجل تنمية الوعي السيبراني، والوعي بالجريمة الألكترونية في الوسط الجامعي الجزائري ولقد فضل الباحث عرض تلك التوصيات في صورة نقاط على النحو التالي :

1. ضرورة زيادة اهتمام الجامعات الجزائرية بالدورات التدريبية في مجال الأمن السيبراني وتقديمها ضمن مشروع تنمية قدرات للمورد البشري للمؤسسة من طلبة، وأعضاء الهيئة التدريسية، والموظفين من خلال عقد دورات تدريبية في تأمين البيانات والخصوصيات على الحاسب والهاتف .

2. عقد دورات في كيفية تعامل مع موقع الويب، ومنصات التواصل الاجتماعي وطريقة استخدام البرامج الحديثة خاص بالأمن السيبراني.

3. عقد ورش عمل وندوات توعية منظمة حول مواضيع الأمن السيبراني والجريمة الألكترونية حيث تكون فرصة لطلبة لتطوير مهاراتهم وتنمية وعيهم عن كيفية التعامل مع المحتوي الرقمي وتجنب الهجمات الألكترونية .

4. تشجيع الطلاب على استخدام كلمات مرور قوية وتغييرها بانتظام وتوفير نصائح حول كيفية إنشاء كلمات مرور آمنة .

5. تشجيع الإبلاغ عن الاختراقات: يجب تشجيع الطلاب على الإبلاغ عن أي اختراقات أو أنشطة غير قانونية تشاهد على الإنترنت. يجب توفير آليات سهلة للإبلاغ .

6. ينبغي تعزيز الوعي حول أنواع الجرائم الإلكتروني المختلفة وكيفية التعرف عليها وتجنبها.

7. التعاون مع مؤسسات أمنية ومتخصصين في أطار تنمية الوعي السيبراني من خلال تنظيم ملتقيات وطنية وزيارات ميدانية للطلاب مع محترفين في مجال الأمان السيبراني ومختصين في مكافحة الجريمة الإلكترونية .

8. تركيز على المشاريع البحثية المتعلقة بالجريمة الألكترونية والوعي سيبراني للتعرف أكثر على ظاهرة من كل الجوانب مما يسهل على السلطات الحكومية الجزائري الحد منها.

المصادروالمراجع

- **القرأن الكريم**
- **الكتب**

1. القاسم. (2003). مداخل الى مناهج البحث العلمي (ب ط). مصر: دار المعرفة الجامعية.

2. أنجريس ترجمة بوفيد صحراوي وكمال بوشرف موريس. (2004). منهجية البحث العلمي في العلوم الإنسانية تدريبات عمالية ، (ب ط). الجزائر: دار القصبة للنشر.

3. عبد الناصر جندلي. ((ب,س,ط)). تقنيات و مناهج البحث العلمي في العلوم السياسية والأجتماعية,(ب,ط). الجزائر: ديوان المطبوعات الجامعية.

4. أحمد ياسين نجلاء . (2014). الرقمنة وتقنياتها في المكتبات العربية. القاهرة: العربي للنشر والتوزيع.

5. 25. مني الأشقر جبور. (2016). السيبرانية هاجسر العصر. جامعة دول العرب: المركز العربي للبحوث القانونية والقضائية.

6. علي راشد. الجامعو التدريس الجامعي. الأردن: دار ومكتبة الهلال – دار الشروق للنشر والتوزيع .، 2008.

7. غياث بوفلجة . التربية والتعليم في الجزائر،ط1. الجزائر: دار الغرب للنشر والتوزيع، 2006.

8. فريد نجار. المعجم الموسوعي لمصطلح التربية ،ط1. بيروت: مكتبة لبنان، 2003.

9. كمال محمود جبرا. التأمين وادارة الخطر. القاهرة: الأكاديميون لنش والتوزيع، 2015.

10. محمد النجار. الثقافة الكمبيوترية للكبار. القاهرة: دار الكتاب المصرية، 2013.

11. ابن منظور. (1971). لسان العرب. بيروت: دار لسان العرب،ج9.

12. قاموس مصطلحات علم الأجتماع. (2003). سلسلة قاموس المنار،(د ط). القاهرة: دار المني.

13. محمد عاطف غيث. (1989). قاموس علم الأجتماع. الاسكندرية: دار المعرفة الجامعية.

14. محمد صالح، و ربيع العجيلي. التعليم العالي في الوطن العربي الواقع واستراتيجيات المستقبل،ط1. عمان، الأردن: دار صفاء للنشر والتوزيع، 2013.

15. محمد مدني أبو ساق. السياسة الجنائية المعاصرة و الشريعة الاسلامية. الجزائر: دار الخلدونية للنشر و التوزيع، 2013.

16. بدران شبل، و كمال نجيب. التعليم الجامعي وتحديات المستقبل. القاهرة، مصر: دارالوفاءللطباعةوالنشر، 2006.

17. رمضان محمد سعودي. الإدارة الجامعية بين رصد الواقع والرؤى المستقبلية، دط. القاهرة: دار المعرفة الجامعية للطباعة والنشر و التوزيع، 2010.

- **المجلات**

18. مل محمد عبد الله البدو. (2021). فعالية المنصات التعليمية في تطبيق التعلم عن بعد بالمرحلة الثانوية بدولة الإمارات(3)،(1). أوراق، الصفحات 175-204.
19. جمال حواوسة. (2018). دور الأسرة في تحقيق الأمن الاجتماعي. مجلةدراسات (7) (3)، الصفحات 136-149.
20. فاروق عزة، و وأخرون. (2020). أمن المعلومات الرقنية وسُبل حمايتها. المجلة المصرية لعلوم المعلومات.7(1)، الصفحات 222-161.
21. فتيحة بوهرين. (2021). الجريمة المعلوماتية في التشريع الجزائري. مجلةالحقوق والعلوم الإنسانية (04) (14)، الصفحات 48-60.
22. أكرم فتحى زيدان وأخرون. (2018). الوعي الأمني لدى عينة من أبناء رجال الشرطة. المجلة العلمية كلية رياض الأطفال(4)(4)، الصفحات 246-272.
23. إيمان بغدادي. (2019). أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية. مجلةأفاق للبحوث والدراسات (04).(2)، الصفحات 184-192.
24. بن عبد الله الحبيب ماجد . (2021). درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية. مجلة العلوم التربوية.1(31)، الصفحات 268-326.
25. حبيب عوفي. (2022). الفضاء الرقمي تحدي أمني جديد واست ا رتيجيات الدول في تحقيق الأمن السيبا رني العالمي. المجلة الجزائر يةٌ للعلوم الإنسانةٌ والاجتماعةٌ .6(1)، الصفحات 102-123.
26. خديجة بغدادي. (2018). الإعلام الأمني ودوره في نشر ثقافة الوعي الأمني المجتمعي. مجلة العلوم الاجتماعية – العدد الرابع يونيو – حُزيران"2018"،، الصفحات 74-86.

27. ر سدوس ، و ع بن السبتي. (2020). المنصة الجزائرية للمجلات العلمية Asjp ودورها في ترقية النشر العلمي الجامعي. Revue des Sciences Humaines & Sociales ,6(1)، الصفحات 238-262.
28. سميرة لالوش. (2021). التعليم عن بعد آلية لضمان جودة العملية التعليمية في الجامعات الجزائرية. جملة البحوث الرتبوية والتعليمية,10(1)، الصفحات 127-142.
29. أمل محمد عبد الله البدو. (2021). فعالية المنصات التعليمية في تطبيق التعلم عن بعد بالمرحلة الثانوية بدولة الإمارات(3)،(1). أوراق، الصفحات 175-204.
30. جمال حواوسة. (2018). دور الأسرة في تحقيق الأمن الاجتماعي. مجلةدراسات (7) (3)، الصفحات 136-149.
31. فاروق عزة، و وأخرون. (2020). أمن المعلومات الرقنية وسُبل حمايتها. المجلة المصرية لعلوم المعلومات.7(1)، الصفحات 222-161.
32. فتيحة بوهرين. (2021). الجريمة المعلوماتية في التشريع الجزائري. مجلةالحقوق والعلوم الإنسانية (04) (14)، الصفحات 48-60.
33. أحمد ياسين نجلاء . (2014). الرقمنة وتقنياتها في المكتبات العربية. القاهرة: العربي للنشر والتوزيع.
34. أكرم فتحى زيدان وأخرون. (2018). الوعي الأمني لدى عينة من أبناء رجال الشرطة. المجلة العلمية كلية رياض الأطفال(4)(4)، الصفحات 246-272.
35. إيمان بغدادي. (2019). أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية. مجلةأفاق للبحوث والدراسات (04).(2)، الصفحات 184-192.
36. بن عبد الله الحبيب ماجد . (2021). درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية. مجلة العلوم التربوية.1(31)، الصفحات 268-326.
37. بن فايز الجحني علي. (2002). الرقابة الإعالمية في وقت الأزمات. أعمال ندوة الإعالم الأمني العربي قضاياه ومشكلاته. الرياض: مركز الدراسات والبحوث.

38. حبيب عوفي. (2022). الفضاء الرقمي تحدي أمني جديد واست ا رتيجيات الدول في تحقيق الأمن السيبا رني العالمي. المجلة الجزائر يةٌ للعلوم الإنسانةٌ والاجتماعةٌ .6(1)، الصفحات 102-123.

39. خديجة بغدادي. (2018). الإعلام الأمني ودوره في نشر ثقافة الوعي الأمني المجتمعي. مجلة العلوم الاجتماعية – العدد الرابع يونيو – حُزيران"2018"،، الصفحات 74-86.

40. ر سدوس ، و ع بن السبتي. (2020). المنصة الجزائرية للمجلات العلمية Asjp ودورها في ترقية النشر العلمي الجامعي. Revue des Sciences Humaines & Sociales ,6(1)، الصفحات 238-262.

41. سميرة لالوش. (2021). التعليم عن بعد آلية لضمان جودة العملية التعليمية في الجامعات الجزائرية. جملة البحوث الرتبوية والتعليمية,10(1)، الصفحات 127-142.

42. سناء إبراهيم أبودوقة . (2013). ضمان الجودة في مؤسسات التعليم العالي في العالم العربي:نظرو مستقبلية (فلسطين دراسة حالة). المؤتمر الدولي لضمان جودة التعليم العالي (الصفحات 2-3). فلسطين: https://site.iugaza.edu.ps/.

43. طواهير وأخرون. (2021). تعتبر هذه المنصة نظام معلوماتي يمكن من تسيير شامل لكل شؤون الجامعة، و يظهر هذا على سبيل المثال لا الحصر في:. مجلة التنمية والاستشراف للبحوث والدراسات,5(2)، الصفحات 30-49.

44. عبد الرحمان أحمد، و محمد فتحي. (2020). استراتجية مقترحة لتحويل جامعة المنيا الى جامعة ذكية في ضوء توجهات التحول الرقمي. مجلة جامعة الفيوم للعلوم التربوية والنفسية.14(6)، الصفحات 628-403.

45. عبير أحمد علي كاعوه. (2020). سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في الخبارات العالمية. دراسات تربوية واجتماعية,26(3)، الصفحات 135-200.

46. ف.رحاب, ع حوتية. (2020). المكتبات الجامعية الرقمية كأنموذج للتحول نحو العمل في البيئة الرقمية. مجلة ببليوفيليا لدراسات المكتبات والمعلومات 2(5)، الصفحات 14-32.

47. فهد بن على الطيار. (2017). دور المدرسة الثانوية في تعزيز الوعي الأمني للوقاية من التطرف الفكري. مجلة كلية التربية، جامعة الأزهر،(36)، (1)، الصفحات 153-208.

48. محمد أحميداتو. (2020). سياسة الرقمنة في قطاع التعليم العالي والبحث العلمي. المجلة الجزائرية للعلوم القانونية، السياسية واالقتصادية 57: ، العدد: خاص، الصفحات 226-244.

49. محمد هبة هاشم . (2020). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعى بمخاطرها وتعزيز قيم المواطنة الرقمية. مجلة كلية التربية.44(3)، الصفحات 81-150.

50. محمد يدو. (2018). متطلبات ضمان جودة التعليم العالي في الجزائر –بين الواقع والاستشراف. معارف 12(23)، الصفحات 400-423.

51. مسعودة طلحة. (2020). الهوية الرقمية "مأزق الاستخدام والخصوصية". مجلة التغير الاجتماعي5(1)، الصفحات 133-154.

52. مني الأشقر جبور. (2016). السيبرانية هاجسر العصر. جامعة دول العرب: المركز العربي للبحوث القانونية والقضائية.

53. نورة عمر الصانع، و وأخرون. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية طلبة من مخاطر الأنترنات. المجمة العلمية لكلية التربية.36(6)، الصفحات 41-90.

54. وأخرون كيحلي. (2017). حتمية تطبيق نظام ضمان الجودة في مؤسسات التعليم العالي في الجزائر نموذج انشاء خلية ضمان جودة التعليم العالي في الجزائر: جامعة الشهيد حمه لخضر الوادي. مجلة الأصيل للبحوث الاقتصادية والإدارية 1(2)، الصفحات 27-54.

55. ولاء محمد الطاهر. (2021). اليات مركز دبى للأمن الإلكتروني للتوعية بالاستراتيجية الوطنية للأمن السيبرانى. مجلة اتحاد الجامعات العربية لبحوث الإعلام وتكنولوجيا الاتصال.1(6)، الصفحات 51-108.

56. طواهير وأخرون. (2021). تعتبر هذه المنصة نظام معلوماتي يمكن من تسيير شامل لكل شؤون الجامعة، و يظهر هذا على سبيل المثال لا الحصر في:. مجلة التنمية والاستشراف للبحوث والدراسات,5(2)، الصفحات 30-49.

57. عبد الرحمان أحمد، و محمد فتحي. (2020). استراتجية مقترحة لتحويل جامعة المنيا الى جامعة ذكية في ضوء توجهات التحول الرقمي. مجلة جامعة الفيوم للعلوم التربوية والنفسية.14(6)، الصفحات 628-403.

58. عبير أحمد علي كاعوه. (2020). سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في الخبارات العالمية. دراسات تربوية واجتماعية,26(3)، الصفحات 135-200.

59. ف.رحاب, ع حوتية. (2020). المكتبات الجامعية الرقمية كأنموذج للتحول نحو العمل في البيئة الرقمية. مجلة ببليوفيليا لدراسات المكتبات والمعلومات 2(5)، الصفحات 14-32.

60. فهد بن على الطيار. (2017). دور المدرسة الثانوية في تعزيز الوعي الأمني للوقاية من التطرف الفكري. مجلة كلية التربية، جامعة الأزهر،(36)، (1)، الصفحات 153-208.

61. محمد أحميداتو. (2020). سياسة الرقمنة في قطاع التعليم العالي والبحث العلمي. المجلة الجزائرية للعلوم القانونية، السياسية واالقتصادية 57: ، العدد: خاص، الصفحات 226-244.

62. محمد هبة هاشم . (2020). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعى بمخاطرها وتعزيز قيم المواطنة الرقمية. مجلة كلية التربية.44(3)، الصفحات 81-150.

63. محمد يدو. (2018). متطلبات ضمان جودة التعليم العالي في الجزائر –بين الواقع والاستشراف. معارف 12(23)، الصفحات 400–423.
64. مسعودة طلحة. (2020). الهوية الرقمية "مأزق الاستخدام والخصوصية". مجلة التغير الاجتماعي5(1)، الصفحات 133–154.
65. أبو الخير, د. ح. م. ط., & طه, د. ح. م. (2023). أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية). المجلة العلمية للدراسات والبحوث المالية والإدارية.71–1 ,(1)15 ,
66. الرشيدي, ع., & المهداوي, ع. (2023). مستوى الوعي بنظام مكافحة الجرائم المعلوماتية لدى طلاب الجامعة. المجلة العربية للدراسات الأمنية, 39(1), 51–63.
67. السعبري, ب. ع., & الزرفي, ع. ع. خ. (2019). انتقال التهديدات من الواقع الى العالم الافتراضي. مجلة جامعة بابل للعلوم الانسانية, 283–298.
68. بنطالب, خ. (2022). التعليم الالكتروني ومعايير الجودة. مجلة منار الشرق للتربية و تكنولوجيا التعليم, 1(2), 16–1.
69. رزقي, ق., & حسين, خ. (2023). الإدارة الالكترونية بين تحديد المفهوم ومتطلبات التطبيق. المجلة الإفريقية للدراسات المتقدمة في العلوم الإنسانية والاجتماعية (AJASHSS), 107–114.
70. محمد أحمد حسن المغربي, أ. (2022). المستودعات الرقمية وأثرها فى تعزيز الاتصال العلمى بالمكتبات الجامعية. المجلة العلمية للمكتبات والوثائق والمعلومات, 4(10), 297–319. https://doi.org/10.21608/jslmf.2022.226661 .
71. أحمد عبد الفتاح الزكي. "دور التعليم الجامعي في خدمة المجتمع بمحافظة دمياط, دراسات تربوية ونفسية." مجلة كلية التربية بالزقازيق 22، رقم 57 (2007): 157–202.
72. اسمهان بن مالك . "خصائص الجريمة المعلوماتية وأسباب إرتكابها." مجلة البيبان للدراسات القانونية والسياسية,(1),(4)، 2019: 102–124.

73. بن علية بن جدو. "تحتديات الامن السيبراني مواجهة الجرايمة الألكترونية." المجلة الجزائرية للأمن الأنساني، 2022: 299-319.

74. حكيم غريب. "الارهاب السيبراني والامن الدولي: التهديدات العالمية الجديدة وأساليب موجهها." المجلة الجزائرية للدراسات السياسية، (5)، (2) ، 2018: 119-104.

75. خالد اسماء، و زهية شابونية. "و ظائف الجامعة الجزائرية مسألة في واقع الفعل و معيقاته." المجلة الجزائرية للأبحاث و الدراسات(2) (6)، 2019: 180-169.

76. عبد المالك بولشفار. "وظائف الجامعة المعاصرة: تحليل نظري لأبرز المقاربات المفسرة." معالم للدراسات القانونية والسياسية، 2018: 334-354.

77. فريدة العلمي ، و رزيقة روابحي . "دور الجامعة : بين جدلية إنتاج املعرفة وتحقيق الاهداف." مجلة ألستاذ الباحث للدراسات القانونية والسياسية(7)(1)، 2017: 207-2019.

78. عبدالسلام محمد المايل، و عادل محمد الشربجي . "الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم- الأسباب-سبُل المكافحة مع التعرض لحالة ليبيا." مجلة أفاق للبحوث والدراسات(4) (1)، 2019: 242-255.

79. محمد رحموني. "خصائص الجريمة و مجالات استخدامها." مجلة الحقيقة,16(3)، 2017: 432-451.

80. مصطفى سعدون، و وأخرون. "الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها"." الكلية التقنيةكركوك، العراق.، 2011: 1-9.

81. مصطفى موسى. "مخاطر تهدد الحق في الخصوصية عبر التقانات الإلكترونية الرقمية." مجلة كلية القانون الكويتية العالمية (22)(11)، 2022: 421-455.

82. نسيمة شمام. "التعليم الالكتروني في الجامعة الجزائرية واقعه وإشكالاته." اللسانيات والترجمة(2) (3)، 2022: 13-30.

83. المطيري, س. ف. س. ا., & ادبيس, س. ف. س. (2023). مفهوم الجرائم الإلكترونية وسماتها. المجلة القانونية, 16(5), 1235– 1274

84. بكوش, & أمين, م. (2022). البعد الجديد للإجرام وخصوصية المجرم الالكتروني. المجلة الجزائرية للحقوق والعلوم السياسية, 7(2), 133–147.

85. خليلـــي, س. (2018). خصوصية المجرم الالكتروني

86. المقصودي, & علي, م. أ. (2017). الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيً

87. ايمان عبد الفتاح عبابنه. (2022). درجة وعي معلمات اللغة العربية للمرحلة الثانوية في الأردن بالأمن السيبراني من وجهة نظرهن وعلاقته ببعض المتغيرات". دراسات، العلوم الإنسانية واالجتماعية، المجّلد ،49 العدد ،5، الصفحات 433-445.

88. ازهرة مولاي. (2012). دور الأستاذ الجامعي في غرس المقاولاتية لدي الطالب الجامعي. مجلة الآداب والعلوم الاجتماعية،()،()، الصفحات 202-188.

89. نهي مصطفي كمال أبو كريشه . (2022). "الوعي المعلوماتي والجريمة الإلكترونية": دراسة لعينة من مستخدمى شبكات التواصل الاجتماعى. مجلة كلية الأدب المجلد 14، العدد 1، الصفحات 2385-2473.

90. الداوي الشيخ، و ليلى بن زرقة. (2015). تطور التعليم العالي في الجزائر خلال فترة 2014/2012. مجلة المؤسسة،(4)،(1)، الصفحات 7-26.

91. الصادق جراية. (2014). تحوّلات مفهوم الأمن في ظلّ التهديدات الدوليّة الجديدة. مجلة العلوم القانونية و السياسية(1)(5)، الصفحات 17-31.

92. الزبن, غ. ب., & الخرابشه, ع. ع. ا. (2021). الجرائم الإلكترونية ومستوى الوعي بخطورتها–دراسة ميدانية على عينة من الشباب الجامعي الأردني. مجلة الجامعة الإسلامية للبحوث الإنسانية, 29.(2)

93. السواط, حمود, ح. ب., الصانع, عمر, ن., أبوعيشة, جميل, ز., سليمان, محمد, إ., عسران, & الدين, ع. س. (2020). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية

والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمى فى التربية, 21(العدد الرابع), 278–306.

94. القحطاني, ع. ا. ب. ح., & حجاب, ع. ا. ب. (2022). درجة الوعي بالأمن السيبراني لدى الأشخاص ذوي الإعاقة البصرية في المملكة العربية السعودية من وجهة نظرهم The degree of cybersecurity awareness among persons with visual impairments in the Kingdom Saudi Arabia from their point of view. مجلة التربية الخاصة والتأهيل, 14(50.2), 1–31

96. الضبان، و وأخرون. (2019). إدمان الطالب على استخدام مواقع التواصل االجتماعي و عالقته بالأمن النفسي والتورط في الجرائم السيبرانية. المجلة الدولية للدراسات التربوية و النفسية(6)(2)، الصفحات 293–267.

- **الأطروحات**

97. رابحي, ع. (2018). الاسرار المعلوماتية وحمايتها الجزائية [أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص]. جامعة أبو بكر بلقايد – تلمسان.

98. غربي, ص. (2014). دور التعليم في تنمية المجتمع المحلي [دكتوراء]. جامعة محمد خيضر.

99. ناصر, ث. (2012). أثبات الجريمة الألكترونية [رسالة دكتوراء]. جامعة نايف العربية للعلوم الأمنية.

- **الملتقيات**

100. بن فايز الجحني علي. (2002). الرقابة الإعالمية في وقت الأزمات. أعمال ندوة الإعالم الأمني العربي قضاياه ومشكلاته. الرياض: مركز الدراسات والبحوث.

101. سناء إبراهيم أبودوقة . (2013). ضمان الجودة في مؤسسات التعليم العالي في العالم العربي:نظرو مستقبلية (فلسطين دراسة حالة). المؤتمر الدولي لضمان جودة التعليم العالي (الصفحات 2-3). فلسطين: https://site.iugaza.edu.ps/.

102. رحيمة نمديلي. "خصوصية الجريمة االلكترونية في القانون الجزائري والقوانين المقارنة." المؤتمر الدولي الرابع عشر حول الجرائم االلكترونية. طرابلس، ليبيا، 2017.

- **المواقع الألكترونية**

103. نوال زايد. (2022). الرقمنة تتغلغل في الجامعة.. وتفرض "مودل" و"بروغرس" على الطلبة والأساتذة. تم الاسترداد من النهار online: https://www.ennaharonline.com/%D8%A7%D9%84%D8%B1%

104. نوال زايد. (2022). الرقمنة تتغلغل في الجامعة.. وتفرض "مودل" و"بروغرس" على الطلبة والأساتذة. تم الاسترداد من النهار online: https://www.ennaharonline.com/%D8%A7%D9%84%D8%B1%/%D9%85%D9%88%D8%AF%D9%84

105. المنتدى الاستراتيجي للسياسات العامة ودراسات التنمية " دراية ". واقع الجرائم الإلكترونية وتداعياتها على المجتمع المصري. 2022. https://draya-eg.org/2022/04/13/%D9%88%D8%A7%D9%82%D8%B9/ (تاريخ الوصول 1 5, 2023).

106. اونلاين الشروق . (2023). الدرك الوطني يكشف عن حصيلة الجرائم الإلكترونية بالجزائر عامي 2022 و2023. جريدة الشروق، 01.

107. حمد الدوسري. (26 كانون الثاني, 2021). نظرية الرابطة التفاضلية لساذرلاند. تم الاسترداد من ملهم:

https://molhem.com/@hamad/%D9%86%D8%B8%D8%B1%D9%8A%D8%A9-

108. ونلاين الشروق . (2023). الدرك الوطني يكشف عن حصيلة الجرائم الإلكترونية بالجزائر عامي 2022 و2023. جريدة الشروق، 01.

- **كتب أجنبية**

109. Cavelty, M. D. (2010). Cyber-security. In The routledge handbook of new security studies (pp. 154–162). Routledge.

110. Picciano, A. G. (2017). Theories and Frameworks for Online Education: Seeking an Integrated Model. Online Learning, 21(3). https://doi.org/10.24059/olj.v21i3.1225

111. Jackson, C. (2010). Network security auditing. Cisco Press.

- **مجلات أجنبية**

112. Canongia, C, & Mandarino, R. (2014). Cyber security the new challenge of the information society. In Crisis Management. Concepts,Methodologies, tools and applications, pp. 60-80.

113. Canongia, C, & Mandarino, R. (2014). Cyber security the new challenge of the information society. In Crisis Management. Concepts,Methodologies, tools and applications, pp. 60-80.

114. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

115. Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. The Internet and Higher Education, 14(1), 44–53.

116. Collis, B., & Smith, C. (n.d.). Desktop multimedia environments to support collaborative distance learning. 30.

117. Cuschieri, S., & Calleja Agius, J. (2020). Spotlight on the shift to remote anatomical teaching during Covid-19 pandemic: Perspectives and experiences from the University of Malta. Anatomical Sciences Education, 13(6), 671–679.

118. D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658.

119. Fast-Berglund, Å., Harlin, U., & Åkerman, M. (2016). Digitalisation of meetings–from white-boards to smart-boards. Procedia CIRP, 41, 1125–1130.

120. Gayness Clark, J., Lang Beebe, N., Williams, K., & Shepherd, L. (2009). Security and privacy governance: Criteria for systems design. Journal of Information Privacy and Security, 5(4), 3–30.

121. Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

122. Guozhu, M., Yang, L., Jie, Z., Pokluda, A., & Boutaba, R. (2015). Collaborative Security: A.

123. Hsu, J. S.-C., & Shih, S.-P. (2015). When does one weight threats more? An integration of regulatory focus theory and protection motivation theory.

124. Ismailova, R., & Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. Information Security Journal: A Global Perspective, 25(1–3), 32–38.

125. Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. International Journal of Computer Networks & Communications (IJCNC) Vol, 9.

126. Paul, P., & Aithal, P. S. (2018). Cyber crime: Challenges, issues, recommendation and suggestion in Indian context. International Journal of Advanced Trends in Engineering and Technology.(IJATET), 3(1), 59–62.

127. Shahimi, S., & Mahzan, N. (2018). Building a Research Model and Hypotheses Development for Internal Audit Consulting: Insights from Literature and Findings of Exploratory Interviews. International Journal of Management Excellence (ISSN: 2292-1648), 10(2), 1257–1283.

128. Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92–100.

129. Stevenson, M., Lai, J. W. M., & Bower, M. (2022). Investigating the pedagogies of screen-sharing in contemporary learning environments—A mixed methods analysis. Journal of Computer Assisted Learning, 38(3), 770–783. https://doi.org/10.1111/jcal.12647

130. Stević, M. P. (2014). Enhancing m-learning using GridFS for storing and streaming digital content. 2(1).

131. Tursunalievich, A. Z., & Rahmat, A. (2021). Challenges In Developing A Digital Educational Environment. Aksara: Jurnal Ilmu Pendidikan Nonformal, 7(2), 247. https://doi.org/10.37905/aksara.7.2.247-254.2021

132. Umarova, Z. (2020). Modern and Innovative Approaches to the Organization of Students' Self-Education in Higher Educational Institutions. Journal La Edusci, 1(4), 5–8.

133. Vedenpää, I., & Lonka, K. (2014). Teachers' and Teacher Students' Conceptions of Learning and Creativity. Creative Education, 05(20), Article 20. https://doi.org/10.4236/ce.2014.520203

134. Watermeyer, R., Crick, T., Knight, C., & Goodall, J. (2021). COVID-19 and digital disruption in UK universities: Afflictions and affordances of emergency online migration. Higher Education, 81(3), 623–641. https://doi.org/10.1007/s10734-020-00561-y

135. Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, 28(1), 167–183.

136. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

137. Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123–147.

138. Alhemeiri, A. A. M., Baharuddin, A. S. B., & Osman, N. Z. (2020)..

139. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

140. ÇAKIR, H., & Ercan, S. (2011). Bilişim Suçları ve Delillendirme Süreci.

141. Dashora, K. (2011). Cyber crime in the society: Problems and preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240–259.

142. Egele, M., Kruegel, C., Kirda, E., Yin, H., & Song, D. (2007). Dynamic spyware analysis.

143. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2, 13–20.

144. Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

145. Igba, I. D., Igba, E. C., Nwambam, A. S., Nnamani, S. C., Egbe, E. U., & Ogodo, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. International Journal of Applied Engineering Research, 13(2), 1144–1154.

146. Arpana, M., Chauhan, M., & Gjimt, P. I. (2012). Preventing cybercrime: A study regarding awareness of cybercrime in Tricity. International Journal of Enterprise Computing and Business Systems, 2(1), 1–10.

147. Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7–9.

148. Mokha, A. K. (2017). A study on awareness of Cyber Crime and security. Research Journal of Humanities and Social Sciences, 8(4), 459–464.

149. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic Sciences, 2(2), 379–398.

150. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

151. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97.

- **أطروحات دكتوراء أجنبية**

152. John, V. J. S. (2021). *The victims' voices: A Routine Activity approach to jail and prison victimization*. City University of New York.

- **ملتقيات أجنبية**

153. Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S., & Yeganeh, E. A. (2010). Definition of spam 2.0: New spamming

boom. *4th IEEE International Conference on Digital Ecosystems and Technologies*, 580–584.

154. Mohamed, L. J. (2016). Aljra'em Alelktrwnyh (Mahytha–Trq Mkafhtha),'. *Eman, Dar Khald Allhyany Llnshr Waltwzy'e*.

- **تقرير أجنبية.**

155. We Are Social & Meltwater (2023). (2023, 2 13). *DIGITAL 2023: ALGERIA*. Retrieved from datareportal: https://datareportal.com/reports/digital-2023-algeria

قائمة الملاحق

الملحق 01: وثيقة لتسهيل عملية توزيع أستبان لدراسة الميدانية مقدمة من طرف عميد الكلية

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
جامعة الجيلالي بونعامة خميس مليانة
كلية العلوم الاجتماعية والإنسانية
الرقم: 47.../ك.ع.إ.إ/ 2023
العمادة

nistère de L'Enseignement Supérieur et de la Recherche Scientifique
Université Djilali Bounaama
Khemis Miliana
Faculty of Social and Human Sciences

خميس مليانة في: 20 مارس 2023

إلى السيّد : نائب العميد المكلف بالبداغوجيا

إلى السادة: رؤساء الأقسام

الموضوع: طلب تسهيل عملية تحضير أطروحة شهادة الدكتوراه للطالب عبد الرزاق برادة

بعد التحية والاحترام

إن الطالب عبد الرزاق براده بصدد تحضير أطروحة دكتوراه في علم الإجتماع، حول موضوع **مستوى الوعي السيبيراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية**، وعليه نرجو من سيادتكم تقديم التسهيلات المكتبية له لإنجاز أطروحته وذلك بتقديم المعطيات والمعلومات المكتبية ،في حدود مايسمح به القانون

وفي الأخير تقبلوا مني فائق التقدير والإحترام

العميد

أ.د. نصر الدين بويحي

الملحق 02: وثيقة تبين حصيلة طلبة المسجلين بكلية العلوم الإنسانية والاجتماعية مقدمة من نائب عميد الكلية.

- جدول رقم 01 يبين حصيلة عدد الطلبة المسجلين في السنة الجامعية الجارية 2022-2023

كلية/ معهد: العلوم الإجتماعية و الإنسانية

السنة الجامعية 2022-2023

ليسانس			ماستر		
المستوى	ذكور	إناث	المستوى	ذكور	إناث
L1	232	801	M1	204	818
L2	187	662	M2	157	518
L3	208	761	المجموع	361	1336
المجموع	627	2224	المجموع العام	1697	
المجموع العام	2851				

- جدول رقم 02 يبين عدد الطلبة المسجلين في السنة الجامعية 2022-2023 حسب الشعب:

كلية/ معهد: العلوم الإجتماعية و الإنسانية

السنة الجامعية 2022-2023

ليسانس				ماستر			
المستوى	ذكور	اناث	المجموع	المستوى	ذكور	اناث	المجموع
L1 قسم العلوم الإنسانية	117	361	478	M1 تاريخ	38	170	208
L1 قسم العلوم الاجتماعية	115	440	555	L2 M1 علوم إنسانية –مكتبات	16	32	48
				M1 إعلام و اتصال	84	265	349
				M1 علم الإجتماع	40	94	134
				M1 علم النفس و التربية	21	192	213
				M1 علوم إجتماعية مختلفة	6	65	71

- جدول رقم 03 يبين عدد الطلبة المسجلين في السنة الجامعية 2022-2023حسب التخصصات:

كلية/ معهد : العلوم الاجتماعية و الإنسانية							
السنة الجامعية 2022-2023							
ليسانس				ماستر			
المستوى	ذكور	اناث	المجموع	المستوى	ذكور	اناث	المجموع
ل1 علوم إنسانية	117	361	478	M1 تاريخ المقاومة و الحركة الوطنية	18	99	117
ل1 علوم إجتماعية	115	440	555	M1 تاريخ الجزائر الحديث	10	35	45
ل1 علوم إنسانية – تكنولوجيا	22	25	47	M1 تاريخ إفريقيا جنوب الصحراء	09	36	45
ل2 علوم إنسانية -مكتبات	22	25	47	M2 تاريخ	23	127	150
ل2 إعلام و اتصال	62	165	227	M2 علوم إنسانية -مكتبات	10	22	32
ل2 تاريخ	16	121	137	M2 إعلام و اتصال	65	180	245
ل2 علم الإجتماع	51	128	179	M2 علم الإجتماع	32	52	84
ل2 علم النفس و التربية	26	194	220	M2 علم النفس و التربية	17	78	95
ل2 علوم إجتماعية -فلسفة	10	29	39	M2 علوم إجتماعية -فلسفة	10	59	69
ل3 علوم إنسانية -مكتبات	17	24	41				
ل3 إعلام و اتصال	91	442	333				
ل3 تاريخ	14	104	118				
ل3 علم الإجتماع	66	166	232				
ل3 علم النفس و التربية	16	192	208				
ل3 علوم إجتماعية -فلسفة	04	33	37				

								المعلومات و التوثيق
310	240	70	M1 إتصال و علاقات عامة					
39	25	14	M1 علم الاتصال الجماهيري و الوسائط الجديدة	227	165	62		L2 إعلام و اتصال
48	32	16	M1 إدارة المؤسسات الوثائقية و المكتبات	137	121	16		L2 تاريخ
134	94	40	M1 علم اجتماع الانحراف و الجريمة	179	128	51		L2 علم الإجتماع
51	47	04	M1 فلسفة تطبيقية	220	194	26		L2 إرشاد و توجيه
20	18	02	M1 فلسفة عربية و إسلامية	39	29	10		L2 علوم إجتماعية فلسفة
213	192	21	M1 توجيه و إرشاد					
116	99	17	M2 تاريخ المقاومة و الحركة الوطنية	41	24	17		L3 علوم إنسانية – تكنولوجيا
20	14	06	M2 تاريخ الجزائر الحديث					المعلومات و التوثيق
14	14	00	M2 تاريخ إفريقيا جنوب الصحراء	27	18	9		L3 إعلام
200	150	50	M2 إتصال و علاقات عامة	306	224	82		L3 اتصال
45	30	15	M2 علم الاتصال الجماهيري و الوسائط الجديدة	118	104	14		L3 تاريخ
32	22	10	M2 إدارة المؤسسات الوثائقية و المكتبات	232	166	66		L3 علم الإجتماع
84	52	32	M2 علم اجتماع الإنحراف والجريمة	208	192	16		L3 إرشاد و توجيه
44	40	04	M2 فلسفة تطبيقية	37	33	04		L3 علوم إجتماعية فلسفة
25	19	06	M2 فلسفة عربية و إسلامية					
95	78	17	M2 توجيه و إرشاد					

الملحق 03: قائمة الأساتذة المحكمين

الرقم	الاسم واللقب	التخصص	الرتبة العلمية
01	سالي مراد	علم الاجتماع جريمة وانحراف	أستاذ التعليم العالي
02	محمد كروم	علم الاجتماع جريمة وانحراف	أستاذ التعليم العالي
03	مغاني مصطفي	علم الاجتماع	أستاذ التعليم العالي
04	قسوم عبد الله	علم الاجتماع	أستاذ التعليم العالي
05	حمرات واليد	علم الاجتماع التربوي	أستاذ التعليم العالي

الملحق 04:الاستبانة في صورتها الأولية الموجهة لتحكيم

بسم الله الرحمن الرحيم

الدكتور/ الأستاذ الفاضل المحترم

تحية طيبة وبعد،

يقوم الباحث بدراسة ميدانية بعنوان "**مستوى وعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية**" وذلك استكمالا لمتطلبات الحصول على درجة الدكتوراه في تخصص علم اجتماع الجريمة والانحراف من جامعة غليزان–الجزائر.

وقد قام الباحث ببناء استبانة لجمع المعلومات المتعلقة بموضوع الدراسة: مكونة من ثلاثة محاور الأول لمعرفة وجهة نظر الطلبة كلية العلوم الإنسانية والاجتماعية لجامعة الجيلالي بونعامة بخميس مليانة حول الوعي السيبراني والجريمة الإلكترونية والمحور الثاني لقياس مستوى وعيهم السيبراني أم المحور الثالث لقياس مستوى اوعيهم بالجريمة الإلكترونية.

وبما إنكم من أهل الخبرة والاختصاص في مجال البحث العلمي فانه من دواعي ارتياح الباحث أن يضع بين أيديكم هاتين الاستبانتين راجيا قراءتها وتحديد أريكم في كل فقرة من فقارات الاستبانتين للتأكد من مدى ملاءمتها.

تقبلوا فائق الاحترام والتقدير.....

اسم الخبير: .....

المرتبة العلمية: .....

الباحث: برادة عبد الرزاق

المحور الأول: الوعي السيبراني والجريمة الالكترونية من منظور الطلبة				
رقم الفقرة	الفقرة	صلاحية الفقرة		التعديل المقترح
		صالحة	غير صالحة	
1	هل تستخدم الأنترانت؟			
2	ماهي عدد الساعات التي تقضيها على الإنترانت؟			
3	ماهي أسباب استخدامك للأنترانت؟			
4	ما مستوي معرفتك بمجال الأمن السيبراني			
5	ما هو الوعي السيبراني في نظرك؟			
6	ما هي الأنشطة التي يجب تتجنبها على الإنترنت لتحافظ على أمانك؟			
7	ما هي الخطوات الأساسية التي تتبعها لتعزيز امنك السيبراني؟			
8	ما هي أهمية الوعي السيبراني في نظرك؟			
9	ما مستوي معرفتك بالجريمة الالكترونية؟			
10	ماهي أكثر الجرائم الالكترونية التي تلاحظها عند استخدامك لمواقع التواصل الاجتماعية؟			
11	هل استخدامك للأنترانت ادي الى وقوعك في الجريمة الالكترونية؟			
12	ماهي الجريمة الالكترونية التي تعرضتا لها؟			
13	هل سبق لك رفع شكوى عند الشرطة بسبب تعرضك للجريمة الالكترونية؟			
14	ماهي الأسباب التي تمنعك من رفعها؟			
15	هل تطالع على قونين الجزائرية للجريمة الألكترونية؟			
16	ماهي معوقات التي تمنعك؟			
17	ماهي العوامل التي تأدي الى وقع في جريمة الإلكترونية؟			
18	ماهي حلول لتنمية الوعي السيبراني للجريمة الالكترونية في الوسط الجامعي في نظرك؟			

المحور الثاني: الوعي السيبراني				
رقم الفقرة	الفقرة	صلاحية الفقرة		التعديل المقترح
		صالحة	غير صالحة	
1	اعتبر الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة			
2	لدي إلمام بمفهوم الوعي السيبراني			
3	اتتبع ممارسات أمان السيبراني الجيدة مثل تجنب فتح رسائل البريد الإلكتروني غير المعروفة			
4	لدي دراية بأهمية الحفاظ على السرية والخصوصية في البيانات الشخصية الحساسة			
5	لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الأنترنت			
6	اخشي على بياناتي الشخصية من انتهاكات الامن السيبراني			
7	لدي اطلاع واسع على الجرائم والهجمات السيبرانية			
8	لدي معوقات شخصية تمنعني من تحقيق الوقاية والامن السيبراني			
9	أقوم بتحديث نظام التشغيل بصورة دورية			
10	أستخدم برنامج للحماية من الفيروسات بصورة مستمرة.			
11	أستخدم جدار الحماية على جهاز الحاسوب وشبكة الخاص بي			
12	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل موافقة			
13	استخدم في جهازي تقنية التحقيق الثنائي			

14	تنظيم حملات توعوية حول التهديدات السيبرانية ينمي الوعي السيبراني لطلبة			
15	التطلع على اخر الاخبار التي تخص مجال الامن السيبراني تنمي الوعي السيبراني لطلبة			
16	تبادل معلومات مع الطلبة حول التهديدات السيبرانية			
17	الحرص على بياناتي الشخصية وعدم مشاركتها مع الغرباء			
18	اعتبر الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة			

المحور الثالث: الوعي بالجريمة الإلكترونية				
رقم الفقرة	**الفقرة**	**صلاحية الفقرة**		**التعديل المقترح**
		صالحة	**غير صالحة**	
1	الجريمة الإلكترونية هي نتاج عن الانتشار الواسع للأنترانت ووسائط الإلكترونية			
2	الجريمة الكترونية عمل إرهابي تعاقب عليه القوانين الدولية			
3	الجريمة الإلكترونية هي كل الأضرار التي تلاحق الطلبة والمؤسسة الجامعية من خلال الوسائل الإلكترونية.			
4	تأدي الجريمة الالكترونية عدم القدرة على الوصول إلى الخدمات الإنترنت			
5	كل ابتزاز او سرقة بيانات في الواقع الافتراضي يعتبر جريمة الكترونية			
6	الجريمة الالكترونية هي كل جريمة كلاسيكية تمارس في الواقع الافتراضي			
7	يوجد قانون مستقل للجريمة الإلكترونية في الجزائر			

8	لدي دراية بقانون العقوبات الخاص بالجريمة الالكترونية في الجزائر			
9	يحد قانون العقوبات الجزائري من وقوع الجرائم الالكترونية			
10	أدرك أهمية الالتزام بالمعايير القانونية عند التوصل الافتراضي			
11	اعرف التعامل مع كل من يحاول إساءة لي عبر الأنترانت			
12	لدي علم بالإجراءات القانونية لتقديم شكوى عند تعرضي لجريمة الكترونية			
13	أدرك خطورة الهجمات الالكترونية على بياناتي الشخصية			
14	أدرك أهمية تحديد وتقييم المخاطر السيبرانية واتخاذ الإجراءات الوقائية المناسبة للحد منها			
15	ان على دراية بأنواع الجريمة المنتشرة في المواقع الافتراضية			
16	تأدي الجريمة الالكترونية الى تشويه سمعة الطلبة في مجتمعهم			
17	تأدي الجريمة الالكترونية الى انتشار الكراهية وفتنة بين الشعوب وبين الشعب الواحد			
18	تسبب الجريمة الالكترونية أضرار بممتلكات الشخصية والمؤسسات الدولة العمومية والخاصة			

الملحق05: الاستبانة في صورتها النهائية

مستوي الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الالكترونية
) (دراسة ميدانية على عينة من طلبة كلية العلوم الإنسانية والاجتماعية بجامعة خميس ـمليانة

الأطروحة مقدمة لنيل شهادة الدكتوراه LMD في تخصص: علم الاجتماع الجريمة والانحراف

لي الشرف أن أضع بين أيديكم هذه الاستمارة كأداة رئيسة لجمع البيانات المتعلقة بدارسة ميدانية حول موضوع الأطروحة المشار إليه أعلاه، لهذا نحن في حاجة لمساعدتكم لكي ننجز عملنا بنجاح، فنرجو من سيادتكم المحترمة التكرم بالإجابة بكل شفافية على الأسئلة هذه الاستمارة بوضع علامة (+) في خانة المناسبة للجواب، كما نود أن نؤكد أن إجابتكم ستحظى بالسرية التامة ولا تستخدم إلا لغرض البحث العلمي.

وفي الأخير تقبلوا فائق عبارات التقدير والامتنان ونشكركم على حسن تعاونكم...

أعداد الطالب الدكتوراه :برادة عبد الرزاق.

الأستاذ المشرف الاول: د. سالي مراد.

الأستاذ المشرف الثاني: د. صيشي يسري.

محور البيانات الديمغرافية:

الجنس : ☐ **ذكر** ☐ **أنثى**

الفئة العمرية : ☐ **من 17-21 سنة** ☐ **من 22-26 سنة** ☐ **27سنة وما فوق**

القسم: ☐ **العلوم الاجتماعية** ☐ **العلوم الانسانية**

المستوي التعليمي : ☐**ليسانس** ☐ **ماستر**

المحور الأول: الوعي السيبراني والجريمة الالكترونية من منظور الطلبة

1. هل تستخدم الأنترانت؟ ☐ دائما ☐أحيانا ☐ نادرا
2. ماهي عدد الساعات التي تقضيها على الإنترانت؟☐أقل من ساعة. ☐ من ساعة الى 3ساعات.

☐ أكثر من 3ساعات.

3. ماهي أسباب استخدامك للأنترانت؟

☐ التعلم

☐ العمل

☐الدردشة وتكوين صدقات

☐ مشاهدة الأفلام والبرامج

☐غير ذالك اذكره .....

4. ما مستوي معرفتك بمجال الأمن السيبراني؟☐منخفض ☐متوسط ☐عالي
5. ما هو الوعي السيبراني في نظرك؟

☐تنفيذ الأنشطة عبر الإنترنت بشكل آمن

☐الوعي بالمخاطر الهجمات الإلكترونية

☐حفاظ على أمن خصوصيات البيانات الشخصية

☐غير ذالك اذكره .....

6. ما هي الأنشطة التي يجب تتجنبها على الإنترنت لتحافظ على أمانك؟

☐الدخول إلى مواقع غير آمنة

☐تحميل الملفات من مصادر غير موثوقة

☐الإفصاح عن معلوماتي شخصية

☐غير ذالك اذكره .....

7. ما هي الخطوات الأساسية التي تتبعها لتعزيز امنك السيبراني؟

☐تحديث البرامج الخاص بجهازي (حاسوب/الهاتف)

☐تجنب فتح رسائل البريد والروابط المجهولة

☐استخدام كلمات مرور قوية ومتنوعة بصفة دورية (البريد الإلكتروني/مواقع التواصل الاجتماعي)

☐ تثبيت برامج المضادة للفيروسات

☐ غير ذالك اذكره .....

8. ما هي أهمية الوعي السيبراني في نظرك؟

☐الحفاظ على سلامة معلوماتي

☐الوقاية من الهجمات والجرائم الإلكترونية

☐زيادة أماني عند استخدام الإنترنت

☐ غير ذالك اذكره .....

9. ما مستوي معرفتك بالجريمة الالكترونية ☐منخفضة ☐متوسطة ☐عالية

10. ماهي أكثر الجرائم الالكترونية التي تلاحظها عند استخدامك لمواقع التواصل الاجتماعية؟

☐التهديد والمضايقة مثل(قرصنة/التنمر /التخويف/الابتزاز)

☐القذف والسب مثل (ترويج أخبار الكاذبة/تقليل من الاحترام/مساس بكرامة)

☐الجرائم غير الأخلاقية مثل (مواقع غير الأخلاقية/صور جنسية)

☐الجرائم المالية (سرقة أرقام بطاقة البنكية/احتيال عند تسوق الإلكتروني)

☐غير ذالك أذكره .....

11. هل استخدامك للأنترانت ادي الى وقوعك في الجريمة الالكترونية؟

☐ تعرضت الى جريمة واحدة

☐ تعرضت الى من جريمتين الى ثلاث جرائم

☐ أكثر من أربع جرائم

12. ماهي الجريمة الالكترونية التي تعرضتا لها؟

☐ قرصنة حساب التوصل الاجتماعي خاص بك

☐انتحال شخصيتك (سرقة بياناتك او صورك)

☐الاحتيال عليك عند التسوق الإلكتروني

☐تعرض لشتم والتهديد

☐أرسال صور وروبط لمواقع غير أخلاقية

☐ غير ذالك اذكره .....

13. هل سبق لك رفع شكوى عند الشرطة بسبب تعرضك للجريمة الالكترونية؟ ☐ نعم ☐لا

☐ في حالة إجابة لا أذكر سبب.....

14. ماهي العوامل التي تأدي الى وقع في جريمة الإلكترونية؟

☐الثقة في الغرباء.

☐غياب المعرفة بالجريمة الإلكترونية.

☐تصفح المواقع الغير الامنة.

☐ غياب المعرفة بمجال الأمن السيبراني

☐ غياب لمعرفة بقوانين التشريعية الجزائرية للجريمة الإلكترونية.

☐غير ذالك اذكره .....

15. ماهي حلول لتنمية الوعي السيبراني للجريمة الالكترونية في الوسط الجامعي في نظرك؟

☐توفير دروس وورش عمل لتدريب الطلاب على الأمن السيبراني

☐تشجيع الإبلاغ عن الحوادث السيبرانية

☐ تنظيم حملات التوعية حول الوعي السيبراني والجريمة الإلكترونية

☐تشجيع الطلبة على حضور الملتقيات الوطنية والدولية حول ظاهرة الجريمة الإلكترونية والوعي السيبراني.

☐غير ذالك اذكره .....

المحور الثاني: الوعي السيبراني

#	السؤال	منخفض جدا	منخفض	متوسط	عالي	عالي جدا
16	اعتبر الوعي السيبراني جزءًا أساسيًا من استخدام الإنترنت بطريقة آمنة					
17	لدي إلمام بمفهوم الوعي السيبراني					
18	اتتبع ممارسات أمان السيبراني الجيدة مثل تجنب فتح رسائل البريد الإلكتروني غير المعروفة					
19	لدي دراية بأهمية الحفاظ على السرية والخصوصية في البيانات الشخصية الحساسة					
20	لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الأنترنت					
21	اخشي على بياناتي الشخصية من انتهاكات الامن السيبراني					
22	لدي اطلاع واسع على الجرائم والهجمات السيبرانية					
23	لدي معوقات شخصية تمنعني من تحقيق الوقاية والامن السيبراني					
24	أقوم بتحديث نظام التشغيل بصورة دورية					
25	أستخدم برنامج للحماية من الفيروسات بصورة مستمرة.					
26	أستخدم جدار الحماية على جهاز الحاسوب وشبكة الخاص بي					
27	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل موافقة					
28	استخدم في جهازي تقنية التحقيق الثنائي					
29	تنظيم حملات توعوية حول التهديدات السيبرانية ينمي الوعي السيبراني لطلبة					
30	التطلع على اخر الاخبار التي تخص مجال الامن السيبراني تنمي الوعي السيبراني لطلبة					
31	تبادل معلومات مع الطلبة حول التهديدات السيبرانية					
32	الحرص على بياناتي الشخصية وعدم مشاركتها مع الغرباء					

المحور الثالث: الوعي بالجريمة الإلكترونية

#	السؤال	منخفض جدا	منخفض	متوسط	عالي	عالي جدا
33	الجريمة الإلكترونية هي نتاج عن الانتشار الواسع للأنترانت ووسائط الإلكترونية					
34	الجريمة الكترونية عمل إرهابي تعاقب عليه القوانين الدولية					
35	الجريمة الإلكترونية هي كل الأضرار التي تلاحق الطلبة والمؤسسة الجامعية من خلال الوسائل الإلكترونية.					
36	تأدي الجريمة الالكترونية عدم القدرة على الوصول إلى الخدمات الإنترنت					
37	كل ابتزاز او سرقة بيانات في الواقع الافتراضي يعتبر جريمة الكترونية					
38	الجريمة الالكترونية هي كل جريمة كلاسيكية تمارس في الواقع الافتراضي					
39	يوجد قانون مستقل للجريمة الإلكترونية في الجزائر					
40	لدي دراية بقانون العقوبات الخاص بالجريمة الالكترونية في الجزائر					
41	يحد قانون العقوبات الجزائري من وقوع الجرائم الالكترونية					
42	أدرك أهمية الالتزام بالمعايير القانونية عند التوصل الافتراضي					
43	اعرف التعامل مع كل من يحاول إساءة لي عبر الأنترانت					
44	لدي علم بالإجراءات القانونية لتقديم شكوى عند تعرضي لجريمة الكترونية					
45	أدرك خطورة الهجمات الالكترونية على بياناتي الشخصية					
46	أدرك أهمية تحديد وتقييم المخاطر السيبرانية واتخاذ الإجراءات الوقائية المناسبة للحد منها					
47	ان على دراية بأنواع الجريمة المنتشرة في المواقع الافتراضية					
48	تأدي الجريمة الالكترونية الى تشويه سمعة الطلبة في مجتمعهم					
49	تأدي الجريمة الالكترونية الى انتشار الكراهية وفتنة بين الشعوب وبين الشعب الواحد					
50	تسبب الجريمة الالكترونية أضرار بممتلكات الشخصية والمؤسسات الدولة العمومية والخاصة					