الجمهورية الجزائرية الديمقراطية الشعبية
جامعة قاصدي مرباح ورقلة
كلية العلوم الإنسانية و الاجتماعية
قسم: علوم الاعلام و الاتصال

مذكرة لاستكمال متطلبات شهادة ماستر اكاديمي

الميدان: العلوم الانسانية

الشعبة: علوم الاعلام و اتصال

التخصص: اتصال جماهيري و الوسائط الجديدة

تحت عنوان :

دور ثقافة امن المعلومات في الحد من مخاطر الجرائم الالكترونية

(دراسة ميدانية طلبة قسم علوم الاعلام و الاتصال)

بوعبون رضوان

جزار حمزة حسام الدين

نوقشت و أجيزت علنا بتاريـــــخ:2023/06/13

أمام اللجنة المتكونة من السادة:

الأستاذ /محرز حمايمي (جامعة قاصدي مرباح .ورقلة) رئيسا

الدكتور / بودربالة عبد القادر (أستاذ محاضر– أ–جامعة قاصدي مرباح. ورقلة) مشرفا ومقررا

الدكتور / قندوز عبد القادر (أستاذ محاضر– أ – جامعة قاصدي مرباح .ورقلة) مناقشا

الموســـم الجامعي: 2022/ 2023

الجمهورية الجزائرية الديمقراطية الشعبية
جامعة قاصدي مرباح ورقلة
كلية العلوم الإنسانية و الاجتماعية
قسم: علوم الاعلام و الاتصال

مذكرة لاستكمال متطلبات شهادة ماستر اكاديمي

الميدان: العلوم الانسانية

الشعبة: علوم الاعلام و اتصال

التخصص: اتصال جماهيري و الوسائط الجديدة

تحت عنوان :

دور ثقافة امن المعلومات في الحد من مخاطر الجرائم الالكترونية

(دراسة ميدانية طلبة قسم علوم الاعلام و الاتصال)

بوعبون رضوان

جزار حمزة حسام الدين

نوقشت و أجيزت علنا بتاريـــــخ:2023/06/13

أمام اللجنة المتكونة من السادة:

الأستاذ /محرز حمايمي (جامعة قاصدي مرباح .ورقلة) رئيسا

الدكتور / بودربالة عبد القادر (أستاذ محاضر– أ–جامعة قاصدي مرباح. ورقلة) مشرفا ومقررا

الدكتور / قندوز عبد القادر (أستاذ محاضر– أ – جامعة قاصدي مرباح .ورقلة) مناقشا

الموســـم الجامعي: 2022/ 2023


بسم الله الرحمن الرحيم

اهداء

أهدي هذا العمل إلى حكمتي وعلمي ..

إلى من أحمل اسمه بكل فخر إلى

أبي العزيز

إلى أمي ..

أطال الله بقاءها وألبسها

ثوب الصحة والعافية إلى من آثروني على نفسهم ..

من علموني الحياة وأظهروا لي ما هو أجمل من الحياة ..

إخوتي

وإلى من كان جنبي طوال المسيرة الدراسية

جزار حمزة حسام الدين

بوعبون رضوان

شكر والتقدير

قبل كل شيء نشكر الله عز و جل و نحمده الذي رزقنا من العلم ما لم نكن نعلم ووهبنا من القوة و الصبر ما نحتاجه للوصول إلى هذا المستوى و إتمام دراستنا و عملنا المتواضع

هذا نفعنا الله به و إياكم كما نتقدم بالشكر الجزيل للأستاذ المشرف الدكتور "**بودربالة عبد القادر**" على التوجيهات و الملاحظات القيمة التي لم يبخل بها علينا، كما نشكره على حسن تواضعه كما نتقدم بالشكر الجزيل لجميع عمال جامعة قاصدي مرباح وقلة.

الملخص:

تهدف هذه الدراسة الى التعرف على دور ثقافة الامن المعلوماتي في الحد من مخاطر الجرائم الالكترونية و التي تمحورت حول التساؤل الرئيسي :**كيف تؤثر ثقافة أمن المعلومات على فهم الطالب لخطورة الجرائم الإلكترونية؟**

ويتفرع منه الأسئلة التالية:

ما هي المصادر المسؤولة عن تشكيل ثقافة أمن المعلوماتي لدى الطلبة الجامعيين بجامعة قاصدي مرباح بورقلة ؟

هل يمتلك الطالب معلومات حول أساليب وطرق الإختراق الإلكتروني؟

هل الطالب على علم بكيفية حماية بياناته على مواقع الويب المختلفة؟

و استنادا الى هذه التساؤلات سعينا لتحقيق مجموعة من الاهداف :

تحديد المصادر التي تساهم في تشكيل ثقافة أمن المعلومات لدى الطلاب.

كشف مدى معرفة الطالب فيما يتعلق بتقنيات وأساليب التطفل الإلكتروني.

التعرف على التقنيات والخطوات التي يتبناها الطلاب لحماية خصوصيتهم على الأجهزة والمواقع الإلكترونية

و قد اعتمدنا على المنهج الوصفي التحليلي و لقد تم الاعتماد على اداة الاستمارة الاستبيان لجمع البيانات من المبحوثين و قد توصلت هذه الدراسة الى مجموعة من النتائج اهمها اكدت الدراسة على وجود ضعف لدى طلبة علوم الاعلام و الاتصال بمفاهيم الامن المعلوماتي و ذلك راجع لنقص الوعي لدى الطلبة ان اغلبية طلبة العينة يعتقدون ان مواقع التواصل الاجتماعي لا تساعد على نشر الوعي بثقافة امن المعلومات ان معظم طلبة العينة لديهم وعي بالإبلاغ عن أي اختراق يحدث، وبشكل خاص إخطار السلطات المسؤولة .

الكلمات المفتاحية: الطلبة ، أمن المعلوماتي ، الثقافة. الجرائم الإلكترونية.

Abstract:

The aim of this study is to identify the role of information security culture in reducing electronic crime risks, which revolves around the main question: How does information security culture affect students' understanding of the dangers of electronic crimes? This leads to the following questions:

What are the sources responsible for shaping the information security culture among university students at Ghardaia University?

Does the student have information about electronic penetration techniques and methods?

Is the student aware of how to protect their data on different websites?

Based on these questions, we sought to achieve a set of goals:

Identifying the sources that contribute to shaping the information security culture among students.

Revealing the extent of the student's knowledge regarding electronic intrusion techniques and methods.
Understanding the technologies and steps that students adopt to protect their privacy on devices and websites.
We relied on the descriptive analytical method and used the questionnaire tool to collect data from the respondents. The study reached a set of results, the most important of which are:
The study confirmed the existence of weakness among communication science and media students in the concepts of information security culture due to the lack of awareness among students.
The majority of the sample students believe that social networking sites do not help spread awareness of information security culture
Most of the sample students are aware of reporting any breach that occurs, especially notifying the responsible authorities.
Keywords: students, information security, culture. Electronic crimes .foreign trade

قائمة المحتويات

قائمة الجداول

قائمة الاشكال

قائمة الملاحق

المقدمة

شهد القرن الحادي والعشرين ثورة متفردة في عالم تكنولوجيا الإعلام والاتصال، إلى درجة أن بعض الخبراء والمختصين صنّفوا المجال المعلوماتي الإلكتروني كـ"الميدان الخامس" للنزاعات. وربما يعود ذلك إلى التطور السريع والانتشار الواسع لهذه التقنية. فقد اعتمدت مختلف مجالات الحياة على الأنظمة الإلكترونية في هذا القرن، خاصةً مع التحول نحو الخدمات الإلكترونية، التي ساهمت بتقليص الجهد والوقت والتكلفة، وساعدت على تلبية الاحتياجات بسرعة ومرونة.

رغم الإيجابيات التي جلبتها شبكة الإنترنت، فقد حملت أيضًا العديد من التهديدات والمخاطر، مثل جرائم الكترونية التي لا تفرق بين الأشخاص والمؤسسات والدول. كما قد تهدد أمن واستقرار الأفراد. إذ لا يتم ذكر دور الإنترنت المتزايد في ذلك. على الرغم من أن المواقع أصبحت وسيلة جذابة للتفاعل والاتصال، وسمة مميزة لحياة المستخدمين في هذا العصر الرقمي، فقد أثرت سلبًا على الخصوصية والأمان، وأصبحت تثير المخاوف في هذا الصدد. إن كل ما ندوّنه وننشره على المنصات الإلكترونية لم يعد خاصًا بنا فحسب، بل أصبح ملكًا عامًا في ظل التدفق الهائل للبيانات. وهذا ما يجعل الأفراد أكثر عرضة للهجمات السيبرانية.

حاولت هذه الدراسة الوقوق على دراية طلبة علوم الاعلام والاتصال بالأمن المعلوماتي، ومدى إدراكهم لأهمية هذا الموضوع، وكيفية مواجهة التهديدات التي يتعرضون لها عبر شبكات التواصل الاجتماعي.

وقد تناولنا في الجانب المنهجي: الإشكالية أهداف الدراسة الأسباب الذاتية والموضوعية لاختيار الموضوع، مرورا بأهمية الدراسة والمفاهيم والمصطلحات، المنهج المتبع للدراسة، عينة الدراسة، أدوت جمع البيانات الدراسات السابقة للاستفادة منها. أما الجانب التطبيقي فقد تناولنا فيه الجانب الميداني للدراسة من خلال عرض البيانات وتحليليها وعرض النتائج التي توصلنا إليها من خلال الإجابة على الأسئلة المدرجة في استمارة البحث.

الاطار المنهجي للدراسة

إشكالية الدراسة:

إن الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا ساهمت و بشكل كبير في تطور معاملات الافراد ، و تسهيليها ذلك في شتى مجالات الحياة المختلفة ؛ لاسيما بعد ظهور الانترنت التي وضعت العالم كله في قرية صغيرة لما ميزها من سرعة في تبادل البيانات و المعلومات ، فتطورت بها المعاملات بين الأفراد ، وكان هذا التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات و الاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد، حيث أصبحت الانترنت من أهم التقنيات التي تساهم في نشر المعارف وتبادل الخبرات في العالم، إذ تعتبر حاليا شريان التواصل بين شعوب العالم، وكذلك مركزا شاملا لمختلف العلوم والمجالات، ولكل الأعمار والمستويات، ونظرا لسهولة الدخول إلى الانترنت من أي مكان واستخدامها عن طريق مختلف الأجهزة كا الكمبيوتر والهواتف النقالة، والأجهزة اللوحية الإلكترونية، أدى هذا إلى انتشارها وتطورها بشكل متسارع وبدأ يظهر للعلن العديد من المشاكل والمخاطر التكنولوجية جراء تفاعل الإنسان مع الانترنت في مختلف مواقعها الالكترونية الشخصية منها، أو الخاصة بالمنظمات الاقتصادية والسياسية ..الخ، حيث تتمثل مخاطرها في القرصنة و التهكير الالكترونيين، بغرض التخريب أو التزوير أو سرقة حقوق الملكية الفكرية وكذلك الاحتيال والتشهير والابتزاز ..الخ.

وكل هذه المخاطر تدخل ضمن ما يصطلح عليه بالجرائم الإلكترونية، التي تمتاز بكونها عابرة للحدود، تحدث في مكان معين، وضحاياها في مكان آخر، إلى جانب السرعة في تنفيذها وإتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين يتمتعون بذكاء خارق وتقنية عالية في التعامل مع التقنية المعلوماتية ويمكن أن يكون للجرائم الإلكترونية عواقب وخيمة ، سواء بالنسبة للأفراد أو المنظمات. يمكن أن يؤدي إلى خسارة مالية ، والإضرار بالسمعة ، وحتى الأذى الجسدي في بعض الحالات.

وفي ظل انتشار هذه المخاطر وغيرها، وجب الاهتمام بها، وإيجاد حلول مناسبة للحفاظ على سرية المعلومات أثناء نشرها وتداولها بين الأفراد، وعليه أصبح من الضروري توفر بعض المهارات والأساليب والقيم والمواقف والسلوكيات التي تشكل كيفية حماية الأفراد لأصول المعلومات الخاصة بهم من الوصول غير المصرح به أو الاستخدام أو الكشف أو التعطيل أو التعديل أو التدمير، وهذا ما يسمى بثقافة الأمن المعلوماتي. إذ يمكن للأفراد تعلم واكتساب العديد من المهارات التي تمكنهم من تفادي أو مواجهة هذه المخاطر، كاستخدام مجموعة من البرامج والتطبيقات التي تكشف أي دخيل وأي ثغرة ، أو صد أي هجمة على الأجهزة ، وذلك با مساهمة ثقافة الأمن المعلوماتي لديهم، في وقت تختلف درجات استخدام التكنولوجيا (الانترنت، مواقع التواصل الاجتماعي..الخ) بين أفراد المجتمع، ومن بينهم فئة الطلبة الجامعيين الذين يشكلون نسبة كبيرة من مستخدمي الانترنت، لحاجتهم المتزايدة لجمع المعلومات من خلالها.

ومن هؤلاء الطلبة نجد طلبة جامعة قاصدي مرباح بورقلة ، الذين بدورهم يستخدمون شتى أنواع التكنولوجيا وتواجههم العديد من المخاطر الأمنية، التي تستوجب عليهم تفاديها عن طريق الوعي الكافي بالأمن المعلوماتي ومنه نطرح الاشكال التالي:

كيف تؤثر ثقافة أمن المعلومات على فهم الطالب لخطورة الجرائم الإلكترونية؟

ويتفرع منه الأسئلة التالية:

1. ما هي المصادر المسؤولة عن تشكيل ثقافة أمن المعلوماتي لدى الطلبة الجامعيين بجامعة قاصدي مرباح بورقلة ؟
2. هل يمتلك الطالب معلومات حول أساليب وطرق الاختراق الإلكتروني؟
3. هل الطالب على علم بكيفية حماية بياناته على مواقع الويب المختلفة؟

أسباب اختيار الموضوع:

إن لكل دراسة علمية أسباب تؤدي بالباحث لدراستها، حيث تنقسم هذه الأسباب إلى ذاتية وموضوعية والتي تظهر كالتالي:

الاسباب ذاتية:

1. الميل الشخصي لدراسة موضوع الامن المعلوماتي لاكتساب ثقافة أوسع في هذا الموضوع.

2. ارتباط الامن المعلوماتي بتكنولوجيا الاتصال والوسائط الجديدة وهو في صميم مجال تخصص الباحثين.

3. الرغبة في تقصي في الوعي الثقافي لطلبة الجامعة في مجال الحماية وأمن المعلومات ، في ضل انتشار العديد من الجرائم الإلكترونية.

الأسباب الموضوعية :

1. خطورة الجرائم الإلكترونية الحالية إلى درجة أنها تشكل تهديدًا لكل من الأفراد والمنظمات ، دون تمييز على أساس مكانتهم الأخلاقية أو الاجتماعية

2. استخدام الطلبة المتزايد لتكنولوجيا و مواقع التواصل الاجتماعي مما يجعلهم أكثر عرضة للهجمات السيبرانية .

3. قلة الدراسات المتعلقة بموضوع الأمن المعلوماتي في قسم علوم الإعلام والاتصال بجامعة ورقلة.

أهداف الدراسة:

سعت هذه الدراسة لتحقيق الأهداف التالية:

1. تحديد المصادر التي تساهم في تشكيل ثقافة أمن المعلومات لدى الطلاب.
2. كشف مدى معرفة الطالب فيما يتعلق بتقنيات وأساليب التطفل الإلكتروني.
3. التعرف على التقنيات والخطوات التي يتبناها الطلاب لحماية خصوصيتهم على الأجهزة والمواقع الإلكترونية.

أهمية الموضوع:

تتجلى أهمية هذه الدراسة من الناحية العلمية من خلال الأهمية البالغة التي يكتسبها الأمن المعلوماتي في الوقت الحالي، حيث أصبحت الجرائم الإلكترونية تهديدا منتشرا للأفراد والشركات والحكومات على حد سواء. أصبح المتسللون ومجرمو الإنترنت متطورين بشكل متزايد في أساليبهم ، مما يجعل من المهم أكثر من أي وقت مضى للأفراد فهم المخاطر وكيفية حماية أنفسهم ومعلوماتهم. ، علاوة على ذلك ، فإن فهم دور ثقافة أمن المعلومات في تثقيف الأفراد حول الجرائم الإلكترونية يمكن أن يساعد المنظمات على خلق ثقافة الأمن داخل أماكن عملهم. ويشمل ذلك تعزيز ثقافة أمنية قوية ، وتوفير التدريب على الأمن السيبراني للموظفين ، وتنفيذ تدابير أمنية فعالة للحد من مخاطر الهجمات الإلكترونية. ، و تعد هذه الدراسة من بين الدرسات الرائدة في قسم الإعلام والاتصال بجامعة ورقلة والتي تتناول هذا الموضوع. أما من الناحية العملية تكمن أهميتها في كونها تهدف إلى تثقيف الأفراد ، وخاصة الطلاب ، حول المخاطر المحتملة التي تأتي مع التطورات التكنولوجية وكيفية التخفيف منها من خلال تبني ممارسات آمنة.

منهج و ادوات الدراسة :

ان اختيار منهج الدراسة في البحوث الاجتماعية و الانسانية يتم وفق الاهداف التي يريد الوصول اليها و هذا انطلاقا من طبيعة الموضوع. فالمنهج هوا عبارة عن مجموعة من العمليات و الخطوات التي يتبعها الباحث بغية تحقيق بحثه[1] كما يعرفه عبد الرحمان بدوي بانه :الطريق المؤدي الى الكشف عن الحقيقة في العلوم بواسطة طائفة من القواعد العامة. تهيمن على يسر العقل و التحديد عملياته حتى يصل الى نتيجة معلومة[2] فالمنهج هوا الطريقة التي يسلكها الباحث للإجابة عن اسئلة التي تثيرها مشكلة الموضوع البحث فعندما يواجه الباحث او الانسان العادي مشكلة فانه يبدا في التفكير كيف يسجل هذه المشكلة و المنهج هو طريق الحل[3]

وقد استخدمنا في درساتنا لهذا الموضوع على المنهج الوصفي التحليلي حيث يعرفه محمد الصاوى محمد مبارك أنه "يقوم هذا المنهج على وصف الظاهرة من الظواهر للوصول إلى أسباب هذه الظاهرة والعوامل التي تتحكم فيها ، و استخلاص النتائج لتعميمها ويتم ذلك وفقا لخطة بحثية معينة ،وذلك من خلال تجميع البيانات وتنظيمها وتحليلها[4] " ،ويعرف أيضا " هو طريقة لوصف الظاهرة المدروسة وتصويرها كميا ,عن طريق جمع معلومات ,مقننة عن المشكلة وتصنيفها ,وتحليلها وإخضاعها للدراسة الدقيقة [5]

تم استخدام هذا المنهج في الدراسة الحالية لأنه يعد الأنسب، كما أنه يساعد على الحصول على معلومات حول ثقافة الطلاب الجامعيين في مجال أمن المعلومات وأساليب تعاملهم بهذا المجال. ويتم تكميم وتحليل البيانات المستخرجة للإجابة على أسئلة الدراسة.

أدوات جمع البيانات:

[1] رشد زواتي . منهجية البحث العلمي في غلوم العلوم الاجتماعية \ اسس علمية و تدريبات \ . دار الكتاب الحديث . القاهرة. 2004. ص 104.

[2] 2003. ص282

احمد بن مرسلي .. مناهج البحث العلمي في الاعلام و الاتصال. ديوان المطبوعات الجامعية . بن عكنون. الجزائر

[3] ابراهيم ابرش. المنهج العلمي و تطبيقاته في العلوم الاجتماعية. دار الشروق لنشر و التوزيع. عمان. ص65

[4] محمد الصاوى محمد مبارك ,البحث العلمي أسسه وطريقة كتابته ,ط1 المكتبة الأكاديمية ,القاهرة ,1992

[5] بلقاسم سلطانية ,حسان الجيلاني , المناهج الأساسية في البحوث الاجتماعية ,ط1,دار الفجر القاهرة ,2012,ص133

يحتاج الباحث لعدة أدوات بحثية يحتاجها في جمع المادة اللازمة لموضوع دراسته حيث تعبر هذه السبل المنتجة لجمع البيانات و المعلومات عن ظاهرة معينة تساعد على انجاز الدراسة وتحقيق الاهداف المنشودة بموضوع البحث، ويجب أن يكون واضحا أن هناك أداة رئيسية يحددها الباحث تكون متوافقة مع المنهج و الطريقة المنهجية المعتمد عليها في الدراسة، ولكن هذا لا يمنع من الاعتماد على اكثر من اداة في جمع المادة حسب ما يتطلبه موقف جمع المادة التي تفيد موضوع الدراسة ، وقد استعنا في هذه الدراسة على الأدوات العلمية التالية:

الاستبيان: يعرفها موريس أنجرس بأنها: "تقنية مباشرة للتقصي العلمي تستعمل إزاء الأفراد، وتسمح باستجوابهم بطريقة موجهة والقيام بسحب كمي بهدف إيجاد علاقات رياضية والقيام بمقارنات رقمية".[6]

أما خالد حامد فعرفها بأنها: " نموذج يضم أسئلة توجه إلى المبحوثين من أجل الحصول على معلومات حول موضوع أو مشكلة أو موقف يتم ملؤها مباشرة وتسمى الاستبيان (Questionnaire) يطلب من المبحوث الإجابة عنها مباشرة ،وقد ترسل عن طريق البريد وتسمى الاستبيان البريدي) Mailed (ques."[7]

تم اختيار استمارة الاستبيان في الدراسة الحالية لأنها تمكن الباحث من جمع أكبر قدر ممكن من المعلومات حول الدراسة من عينة كبيرة نوعا ما وتسمح باختصار الجهد والوقت ،و تمكن كذلك من الكشف عن الاختلافات في إجابات المبحوثين في إطار الظاهرة المدروسة. ومن هنا لقد قمنا ببناء استمارة الاستبيان لجمع المعلومات والمعطيات من أن افرد العينة وبناء على محاور الدراسة التي تحتوي على 3 محاور رئيسية وقمنا بتقسيمها كالتالي:

أولا : البيانات الشخصية : لأن افراد العينة وقد احتوت على البيانات الشخصية من الجنس والسن.

من ثم احتوى على المحاور الاساسية في الاستبانة وكانت كالتالي:

المحور الأول: تناول المصادر المسؤولة عن تشكيل ثقافة أمن المعلومات لدى الطلاب الجامعيين لمساعدة في التعرف على المصادر التي يتلقى منها الطلاب المعلومات والإرشادات حول أمن المعلومات.

المحور الثاني: احتوى هذا المحور اسئلة تهدف الى معرفة مدى معرفة الطالب على اساليب و طرق الاختراق الالكتروني بهدف التصدي لهذه الاساليب و البرمجيات الخبيثة

المحور الثالث: كان هدفنا من اسئلة هذا المحور هو الوصول لمدى معرفة الطالب لكيفية حماية بياناته على مواقع الويب المختلفة و لإجراءات اللازمة لحماية بياناته الشخصية

الجدول رقم 01 : يوضح الاساتذة المحكمين

[6] موريس أنجرس، منهجية البحث العلمي في العلوم الإنسانية تدريبات علمية، ط2، تر: بوزيد صحراوي وآخرون، دار القصبة للنشر، الجزائر، 2006،ص 204.

[7] نادية سعيد عيشور، منهجية البحث العلمي في العلوم الاجتماعية، مؤسسة حسين رأس الجبل للنشر، الجزائر، 2017، ص 352.

اسم الاستاذ	الدرجة العلمية
د :تومي فضيلة	استاذة تعليم العالي جامعة ورقلة
أ :صانع رابح	استاذ مساعد جامعة ورقلة
د :ليليا بوسجرة	استاذ محاضر المدرسة العليا لصحافة و الاعلام

قياس ثبات الاستبيان: لمعرفة مدى ثبات الاستبيان وفقراته استخدمنا مقياس ألفاكرومباخ الذي يأخذ قيمة بين 0 و1 حيث كلما اقتربت القيمة إلى الواحد(1) كان هناك ثبات للفقرات والعكس كلما اقتربت القيمة إلى الصفر (0).

الجدول التالي يوضح كيفية حساب معامل الصدق والثبات لمحاور الاستبيان:

الجدول رقم 02 : يوضح معامل الثبات للإستبيان

الرقم	عدد الفقرات	الفا–كرومباخ
01	المصادر المسؤولة عن تشكيل ثقافة أمن المعلوماتي لدى الطلبة الجامعيين	-0,081
02	مدى إطلاع الطالب على أساليب وطرق الاختراق الالكتروني	-1,130
03	معرفة الطالب بكيفية حماية بياناته على مواقع الويب المختلفة	0,649
كل المحاور		3220.

المصدر: مخرجات SPSS

صدق الاستبيان هو الجذر التربيعي للثبات ويساوي 0,322 نلاحظ من خلال الجدول أن قيمة معامل ألفا–كرومباخ بلغت 0,322 وتعتبر قيمة جيدة ومقبولة، مما يدل على أنه في حالة توزيع نفس الاستبيان على نفس العينة في نفس الظروف السابقة فإن 32% من العينة ستكون لهم نفس الإجابات كذلك بالنسبة لمعامل الصدق لجميع فقرات ومحاور الاستبيان الذي بلغ 0,322 وعليه يتحقق ثبات الاتساق الداخلي للمقاييس المستعملة وبالتالي يمكن اعتماد هذه الأداة في الدراسة.

مجالات الدراسة :

يعد تحديد مجالات الدراسة أمرًا حاسمًا في بناء المنهجية لأي موضوع؛ حيث يزود الباحث بالمعلومات اللازمة التي تساعده على تفسير وتحليل ميدان الدراسة، ويشمل ذلك النطاق الزمني والجغرافي والبشري الذي يتم فيه الدراسة. ويختلف تحديد هذه المجالات الرئيسية باختلاف أنواع الدراسات والبحوث.

المجال المكاني:

أجريت هذه الدراسة بجامعة قاصدي مرباح ورقلة بمدينة ورقلة التي تأسست في 22مارس1982وأقيمت بمرسوم رقم 65-88 المؤرخ في 22مارس1988،وبالضبط بكلية العلوم الإنسانية والاجتماعية- قسم علوم الإعلام والاتصال.

المجال الزماني: وقد تطرقنا الى موضوعنا الذي هو بعنوان " دور ثقافة الامن المعلوماتي في الحد من مخاطر الجرائم الالكترونية " على مرحلتين:

المرحلة الاولى :من اكتوبر 2022 الى مارس 2023.

- ✓ ضبط متغيرات الدراسات السابقة المتعلقة بالموضوع
- ✓ الانطلاق بصياغة العناصر المنهجية المتعلقة بالموضوع

المرحلة الثانية :من مارس 2023 الى جوان 2023

- ✓ اجراء الدراسة الميدانية من توزيع الاستبيان و تفريع المعطيات ثم تحليل البيانات وصولا الى نتائج عامة

المجال البشري: يتمثل المجتمع الأصلي لهذه الدراسة في طلبة قسم علوم الإعلام بجامعة قاصدي مرباح ورقلة خلال الموسم الجامعي 2022-2023، وعددهم 1223 طالب من قسم علوم الإعلام والاتصال، والذي انتقينا منه عينة قدرت بـ 125 مفردة.

الدارسات السابقة

من أهم المصادر الأساسية في عملية البحث العلمي والتي تعد ركيزة أساسية في اتمام الباحث لموضوعه هي الدراسات السابقة، في تعد بمثابة امتداد علمي للموضوع والتي يحاول الباحث منها تجنب الأخطاء واستقاء الافكار والمعلومات وعلى هذا الأساس وفي إطار دراستنا قمنا بتفحص بعض المذكرات الى أننا لاحظنا أن هذا الموضوع لم يلق اهتمام من الطلبة الباحثين وقد اعتمدنا على هذه الدراسات.

الدراسة الاولى : بعنوان " دور الامن المعلوماتي في الحد من الجريمة المعلوماتية " مذكرة مكملة لنيل شهادة الماستر في قسم الحقوق تخصص " قانون جنائي " للباحث " علاوي محمد " بجامعة محمد خيضر بسكرة، سنة 2017/2016. صاغ الباحث الاشكالية في التساؤل الرئيسي التالي: ما هي اليات مكافحة الجريمة المعلوماتية؟

وقد تفرعت منه التساؤلات الفرعية التالية:

- ✓ هل يمكننا اعطاء تعريف جامع مانع للجريمة المعلوماتية؟
- ✓ هل ان الجريمة المعلوماتية تشترك من حيث الاركان مع الجريمة التقلدية؟

- ✓ كيف واجه المشرع الجزائري هذه الجريمة؟

واعتمد الباحث على المنهج الوصفي التحليلي، وتحليل أهم النصوص القانونية المنظمة للجريمة المعلوماتية في التشريع الجزائري وقد قسم الموضوع إلى فصلين حيث تناول في الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية ثم تطرق الى آليات مواجهة الجريمة المعلوماتية وتوصل الباحث على مجموعة من النتائج أهمها:

- ✓ **بالنسبة لتعريف الجريمة** :تبين أن كل الإعمال والأنشطة الإجرامية متى مست المكونات المادية أو المعنوية لنظام المعلومات وألحقت إضرار بأشخاص عدت جريمة معلوماتية إلا انه لا يوجد إجماع على تعريف موحد للجريمة المعلوماتية حتى قيل أنها تقاوم التعريف

- ✓ **بالنسبة للحماية الجنائية:** فكرة الحكومة المستحدثة التي تقوم أساسا على توفير الحماية الجنائية للمعاملات الالكترونية و الهدف من إنشاها هو ربط المواطن بأجهزة الحكومة للحصول على الخدمات بشكل آلي وتخفض كلفة المعاملات الإدارية ويسرع في وتيرتها ولحسن أداءها ولن يأتي ذلك مالم تكن هناك حماية قانونية تجرم الاعتداء على كل المعاملات

- ✓ **بالنسبة للنصوص المستحدثة:**

- فما يتعلق بالنصوص المستحدثة في هذا المجال فإن أهم نتيجة تمحص عنها هو الاعتراف الضمني للمشرع الجزائري عن مالية المكونات المعنوية لنظام المعلوماتي لحماية أنظمة المعالجة الآلية للمعطيات ، وبتعديله لقانون العقوبات ونصه على تجريم الدخول والبقاء دون إذن في نظام المعالجة الآلية للمعطيات وذلك دون التطرق لبعض الجرائم الأخرى كالسرقة أو النصب مرده أن جريمة الدخول والبقاء غير المشروع هي بوابة أغلب الجرائم الواقعة في مجالات المعاملات الالكترونية ، فاختلاس المعلومات أو إتلافها أو الاحتيال للحصول عليها لا يتم إلا بدخول في النظام المعلوماتي وبتجريم الدخول الغير المشروع يكون المشرع غلق باب وقوع جرائم أخرى .

- كما تبين لنا وجود قصور في النصوص المستحدثة فيما تعلق بالمساس بأنظمة المعالجة الآلية للمعطيات حيث أنها لا تكفل المعاملات الالكترونية بحماية جنائية من كل جوانب بل تحميها من بعض الاعتداءات دون الأخرى .

الدراسة الثانية :بعنوان " الابتزاز الالكتروني و انحراف الفتيات " مذكرة مكملة لنيل شهادة الماستر في علم الاجتماع تخصص " جريمة و انحراف " للباحثتين " طراد دنيا " و" عمراني هيام " بجامعة العربي التبسي تبسة، سنة 2022/2021. صاغت الباحثتين الاشكالية في التساؤل الرئيسي التالي: الى اي مدى يمكن للابتزاز الالكتروني ان يؤثر على الفتيات و يدفعهن للانحراف؟

وقد تفرعت منه التساؤلات الفرعية التالية:

- ✓ هل هناك علاقة بين الابتزاز الالكتروني و انحراف الفتيات؟

- ✓ هل يؤثر الابتزاز الالكتروني على انحراف الفتيات؟

- ✓ هل مظاهر انحراف الفتيات تؤدي الى ابتزازها الكترونيا؟

واعتمدت الباحثتين على المنهج الوصفي و المنهج الاحصائي، ووظفتا أداة الملاحظة و استمارة البحث، وقد اعتمدوا في الملاحظة على المعاينة الشاملة و الدقيقة في كلية العلوم الانسانية و الاجتماعية بجامعة العربي التبسي . اما في استمارة البحث استخدمت العينة العشوائية ممثلة في 136 مفردة، من طالبات كلية العلوم الاجتماعية و الانسانية بجامعة تبسة وتوصلت الباحثتين على مجموعة من النتائج أهمها:

- ✓ معظم الفتيات يتقن في الأشخاص المتعاملين معهم في الوسط الافتراضي نتيجة تحققهن من هويتهم قبل قبول صداقتهم أو على دراجة قرابة بهن.
- ✓ الفتيات يتعاملن مع أصدقائهن في الوسط الافتراضي باستخدام الصوت والصورة والفيديو والكتابة بنسبة قليلة.
- ✓ الفتيات على مستوى كلية العلوم الإنسانية والاجتماعية لم يتعرض إلى ابتزاز إلكتروني وهذا ولا ينفي وجود نسبة مقبولة من اللاتي تعرض للابتزاز نتيجة نقص الرقابة الأسرية
- ✓ تعرض الفتيات إلى الإبتزاز الإلكتروني من خلال أصدقائهن أي أقرب الناس إليهم بعد أسرهم أكثر أنواع الابتزاز الإلكتروني الذي يقع على الفتيات هو جنسي بالدرجة الأولى ومادي بالدرجة الثانية أول جهة تلجأ إليها الفتات التي وقعت ضحية ابتزاز الكتروني هي . طلب المساعدة سرا من شخص موثوق به دون اللجوء لا إلى أهلها و / أو الشرطة
- ✓ عدم سلوك مجتمع الدراسة الإنحرافي بالتوجه إلى التدخين وهذا يرجع إلى أن التدخين من سلوك الرجال.
- ✓ لا تحضر جلسات تعاطي المخدرات وهذا يرجع إلى أن مثل هذا السلوك يجعلها في موضع شبها وتشويه لسمعتها وسمعة عائلتها.
- ✓ إن الفتيات لا يلبس البسة فاضحة تجعلهم عرضة لأنواع الابتزاز والتنمر من قبل الأفراد وهذا ما يدل على مدى التزامهن وتربيتهن الحسنة خوفا على أنفسهم بالدرجة الاولى و خوفا من سمعة اهليها بالدرجة الثانية .
- ✓ إن الفتيات لا يقبلن الخروج مع شخص في علاقة حميمية غير شرعية بل يفضلن العلاقات الشرعية. لا تضطر الفتيات إلى اللجوء إلى السرقة أن سنحت لها الفرصة، ويرجع ذلك للأسباب السابقة والفرضية السابقة المدرجة ضمن الجدول المتعلق بتعاطي الممنوعات
- ✓ الفتيات يتبادلن صور وفيديوهات شخصية فاضحة مع أصدقائهم وهذا دافع لإختراق المبتز حسابهم واستغلالها في تطبيع أنواع الإبتزاز التي يفضلها عليهن
- ✓ من أهم المصادر الأساسية في عملية البحث العلمي والتي تعد ركيزة أساسية في اتمام الباحث لموضوعه هي الدراسات السابقة، في تعد بمثابة امتداد علمي للموضوع والتي يحاول الباحث منها تجنب الأخطاء واستقاء الافكار والمعلومات وعلى

هذا الأساس وفي إطار دراستنا قمنا بتفحص بعض المذكرات الى أننا لاحظنا أن هذا الموضوع لم يلق اهتمام من الطلبة الباحثين وقد اعتمدنا على هذه الدراسات.

الدراسة الثالثة : بعنوان " الجريمة الالكترونية و اجراءات مواجهتها " مذكرة مكملة لنيل شهادة الماستر في قسم الحقوق تخصص " قانون جنائي " للباحثين " شاهين خضر " و " رضوان السعادة " بجامعة محمد بوضياف المسيلة، سنة 2021/2020. صاغ الباحثين الاشكالية في التساؤل الرئيسي التالي: ما هي الجريمة الالكترونية و اليات مواجهتها؟

واعتمد الباحثين على المنهج الوصفي حيث قام بوصف الجريمة الالكترونية ثم المنهج التحليلي و ذلك بتوضيح المفاهيم الخاصة با الجريمة الالكترونية و تحليلها ثم المنهج المقارن وتوصل الباحثين على مجموعة من النتائج أهمها:

- ✓ الحاسوب هو أساس ارتكاب الجريمة الإلكترونية.
- ✓ أهم دوافع ارتكاب الجريمة الإلكترونية هو تحقيق عائد مادي.
- ✓ الجريمة الإلكترونية لا تتسم بالعنف في ارتكابها. الجريمة الإلكترونية ظاهرة حديثة وبالتالي يمكن ظهور أنواع أخرى من الجرائم المعلوماتية.
- ✓ عجز التشريعات عن مكافحة الجريمة الإلكترونية بما فيها التشريع الجزائري يؤدي إلى إفلات مرتكب الجريمة من العقاب.
- ✓ أبرز التحديات التي تثيرها الجريمة الإلكترونية من الناحية القانونية هو تنازع الاختصاص والقانون الواجب التطبيق.

الدراسة الرابعة : بعنوان " نظام امن المعلومات في الجزائر " مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية و العلاقات الدولية تخصص " سياسات عامة و ادارة محلية " للباحثة " حمودي كاهنة " بجامعة مولود معمري تيزي وزو، سنة 2017/2016. صاغت الباحثة الاشكالية في التساؤل الرئيسي التالي: ما مدى مساهمة نظام المعلومات في مواجهة مخاطر نظام المعلومات في الجزائر بصفة عامة و في بلدية سوق الاثنين بولاية تيزي وزو بصفة خاصة؟

وقد تفرعت منه التساؤلات الفرعية التالية:

- ✓ ما هي المخاطر التي تواجه نظام المعلومات؟
- ✓ ما هي الإستراتيجية الأمنية المنتهجة للحد من انتشار هذه المخاطر؟
- ✓ ما هي السياسة الأمنية التي تعتمدها الإدارة العامة؟
- ✓ فيما تتمثل أهم القوانين والجهود الدولية والجزائرية في مجال نظام أمن المعلومات؟
- ✓ ماهو واقع نظام أمن المعلومات في بلدية سوق الاثنين ولاية تيزي وزو؟

واعتمدت الباحثة على المنهج الوصفي و منهج دراسة الحالة، ووظفت أداة الملاحظة و المقابلة، وقد استخدمت الملاحظة في مصالح البلدية لمتابعة طريقة سير العمل داخل الإدارة والعمل الذي تقوم به مهندسة الإعلام الآلي في تنفيذ السياسة الأمنية الخاصة بالبلدية. اما في المقابلة فتمحورت مع الأمين العام للبلدية والمكلفة بالإعلام الآلي لتقديم استفسارات حول واقع نظام أمن المعلومات بالبلدية وتوصلت الباحثتين على مجموعة من النتائج أهمها:

- ✓ ان نظام أمن المعلومات ونتائج كل من المقابلة والملاحظة والتي أضفت على إبراز الايجابيات التي تعود للنظام من سرعة التنفيذ وكذا سهولة مراقبة أعمال المصالح بالإضافة إلى أنه يساعد على اتخاذ القرارات والتدابير اللازمة لمواجهة أي خطر محدق من خلال استعمال ملحق النظام وتطبيقه.
- ✓ كما يقوم باختبار صحة الفرضيات المبنية وكذا الإجابة على الإشكالية الرئيسية والتي تبين كفاءة و فعالية نظام أمن المعلومات في المؤسسة.

نلاحظ ان اغلب الدراسات السابقة استخدمت المنهج الوصفي الذي يساعد في التقصي و يستخدم في البحوث الانسانية والاجتماعية لرصد دور ثقافة امن المعلومات ،كما نلاحظ ان العينات المستخدمة لديهم منها العينات العشوائية و منها العينات القصدية على حسب ما يخدم اهداف الدراسة اما من خلال ادوات الدراسة فقد استخدموا الاستبيان. الملاحظة و المقابلة في كافة دراستهم و بالرغم من اختلاف الدارسات و التنوع الا اننا حولنا الاستفادة منها قدر المستطاع من خلال طريقة المنهجية و التقارب في موضوع الدراسة كما اننا حاولنا قدر المستطاع محاولة. تقديم دراسة علمية معتمدة على التراكمية السابقة من الدارسات التي اجريت في نطاق دور ثقافة امن المعلومات في الحد من الجريمة الالكترونية.

و قد قامت الدارسات السابقة بمعالجة الجوانب الفنية لأمن المعلومات. ركزت على الأدوات والتقنيات المستخدمة لحماية الأنظمة والبيانات الرقمية ،بينما حاولنا التطرق لهذا الموضوع من الجانب الثقافي في مواقف ومعتقدات وسلوكيات الأفراد والمنظمات تجاه أمن المعلومات. تقر بأن الانتهاكات الأمنية غالبًا ما تنتج عن خطأ بشري أو إهمال ، وأن معالجة ذلك يتطلب فهم العوامل الاجتماعية والثقافية التي تؤثر على تصرفات الناس. من خلال دراسة ثقافة أمن المعلومات ، يمكننا تطوير استراتيجيات أكثر فاعلية واستدامة لحماية المعلومات الحساسة ، سواء في حياتنا الشخصية أو داخل المنظمات.

تحديد مفاهيم الدراسة :

أ. الدور:

- ✓ **لغة:** يمكن فهم كلمة الدور بدلالة الحركة في محيط أو بيئة معينة من الفعل، دار، دورا، دورانا بمعنى طاف حول الشيء ويقال ايضا دار ،حوله، وبه، وعليه وعاد إلى الموضع الذي ابتدأ منه.[8]

[8] جابو ربي مصطفى، المعج الوسيط، المكتبة الاسلامية للطباعة والنشر، القاهرة، 1972 ، ص 302

- ✓ **اصطلاحا** يعرف على انه المركز او المنصب الذي يحتله الفرد أو الذي يحدد وجباته وحقوقه الاجتماعية كما هو السلوك المتوقع من شاغل الأول هي المركز الاجتماعي، والمركز الاجتماعي هو العلاقة او الاشارة التي تحدد طبيعة الدور الاجتماعي مما يدل على ان هناك علاقة وثيقة بين الدور الاجتماعي والمركز الاجتماعي ودور الاعلام عموما في المجتمع ينطلق من مجموعة المهام التي يحددها له المركز و وظيفة في المجتمع بصفة تضم مجموعة من الأفراد يقومون بمجموعة ادوار في الاطار الاعلامي والقانون الاجتماعي والاقتصادي. 2

- ✓ **التعريف الاجرائي** : يمكننا مما سبق أن نعرف الدور هو تلك العملية التي ترتبط بالأفراد وبواجباتهم تجاه المجتمع ويعتبر الدور هو الوسيلة الذي تمكن الفرد من تحديد مركزه في المجتمع من خلال مجموعة المهام الذي يقوم بها.

يمكننا مما سبق أن نعرف الدور انه العلاقة التي تربط بين الأفراد وواجباتهم تجاه المجتمع، حيث يساعدهم هذا على تحديد موقعهم في المجتمع وذلك من خلال القيام بمجموعة من المهام المحددة."

ب. الثقافة:

- ✓ **لغة:** ثَقِفَ* ـ و ثَقُفَ ـ ثَقْفًا وثَقَفًا وثَقَافَةً: صار حاذقًا خفيفًا فهو ثَقْفٌ وثَقُفٌ وثَقِفٌ وثَقِيفٌ . ثَقِفَ* ـ ثقْفًا وثَقَافَةً وثُقُوفَةً الكلام حَذِقه وفهمهُ بسرعةٍ، وثَقْفًا: غلبه في الحذق، ثاقفَه: غالبه في الحذق. يقال "ثاقفه فثقفه" أي غالبه فغلبه[9].

- ✓ **اصطلاحا:** أبرز التعريفات الغربية للثقافة الذي تردد صداه لدى الغربيين ثم لدى العرب كثيرا هو تعريف "إدوارد تايلر" عام 1871 في كتابه "الثقافة البدائية" الذي يقول فيه أن الثقافة هي: " ذلك الكل المركب –بعض الترجمات تقول المعقد– الذي يضم المعرفة، والمعتقدات، والفن، والأخلاق، والقانون، والتقاليد، وكل العادات والقدرات التي يكتسبها الإنسان من حيث هو عضو في المجتمع".[10]

- ✓ **إجرائيا:** الثقافة هي مفهوم أساسي يشكل هوية الفرد ومعتقداته. يتطور بمرور الوقت ويختلف باختلاف مجموعات الأشخاص. من أجل التواصل والتفاعل بشكل فعال مع الآخرين ، يحتاج الأفراد إلى تطوير فهم للثقافات المختلفة والانفتاح على تعلم أشياء جديدة. على سبيل المثال ، تشير الثقافة الصحية إلى معرفة الفرد ووعيه بمختلف جوانب الصحة ، فضلاً عن قدرته على التنقل والحفاظ على بيئة صحية.

ت. الأمن:

- ✓ **لغة:** " (**أمن**) الأمان و الأمانة بمعنى وقد أمنت فأنا آمن وآمنت غيري من الأمن والأمان والأمن ضد الخوف ، والأمانة ضد الخيانة ".[11]

[9] المنجد في اللغة و الأعلام ،ط43، دار المشرق ،لبنان،2008،ص71

[10] عبد الرحمن بن زيد الزنيدي، المثقف العربي بين العصرانية والإسلامية، ط1، دار كنوز اشبيليا للنشر، الرياض، السعودية، 2009، ص 13.

[11] إبن المنظور ،لسان العرب ،جزء 16، وزارة الشؤون الإسلامية والأوقاف و الدعوة و الإرشاد، السعودية ،ص160

- ✓ **المعلومات لغة:** مشتقة من المصدر "**علم**" وبهذا الاشتقاق تكون وثيقة الصلة بالعلم والمعرفة والتعليم والتعلم والدراية والإحاطة و الادراك والمعرفة والوعي و الإعلام،وبالانجليزية **information** وهذه الكلمة مشتقة أصلا من اللاتينية ، وكانت تعني عملية الاتصال أو ما يتم إيصاله أو تلقيه [12].

ث. الأمن المعلوماتي:

- ✓ **اصطلاحا:** يعرف بأنه حماية نظام المعلومات من التهديدات المقصودة وغير المقصودة وللقيام بهذه المهمة يجب تحديد مكونات النظام والتهديدات و اتخاذ الإجراءات المناسبة لمنع هذه التهديدات أو التقليل من ضررها على المؤسسة[13].
- ✓ **إجرائيا:** تعريف الأمن المعلوماتي يشير إلى ضرورة حماية خصوصية الفرد وحمايتها من أي نوع من التهديدات والمخاطر، وهذه الأضرار يمكن أن تختلف حسب طبيعة التعامل مع البيانات، سواء كانت عمليات اختراق أو سرقة للبيانات أو أي ضرر تقني أو فني ناتج عن الأعطال في الحاسوب أو الجهاز المستخدم.

ج. الجريمة الالكترونية :

- ✓ **الجريمة لغة** : ماخوذة من الجرم و هي الذنب و الجناية جمعها جرائم و جرم الشيئ قطعه و جرمه الرجل على قومه واليهم. ذنب و جنى جنتئة[14]
- ✓ **اصطلاحا:** معظم الفقهاء و المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه الى ما قرره الموارديي في الاحكام السلطانية بقوله : الجرائم محظورات شرعية زجر الله عنها بحد او تعزيز يعني اذا كانت ممن يتعمد ارتكابها. اما الامام ابو زهرة فبعدها ذكر تعريف الماوردي و ايده ساق من بين نصوصه تعريف اخر للجريمة فقال 'هي المعصية التي يكون فيها عقاب يقرره[15]
- ✓ **إجرائيا:** وفي الدراسة الحالية يقصد به ذلك الطالب الجامعي المنتمي لقسم علوم الإعلام والاتصال أو قسم الإعلام الآلي وتكنولوجيا المعلومات ،بجامعة قاصدي مرباح – ورقلة ،و الذي يفترض فيه أن يتمتع بالقدرات والكفاءات الفكرية والوعي الكافي في مجال الأمن المعلوماتي وكيفية حماية نفسه من المخاطر الناجمة من كل أنواع المشاكل الالكترونية سواء كانت تتعلق بأجهزته أو حساباته الخاصة في المواقع المختلفة.

---

[12] زهرة بزاوية ،مجتمع المعلومات والكفاءات الجديدة لدى أخصائي المعلومات،"دراسة ميدانية بالمؤسسات الوثائيقية لولاية وهران" مذكرة لينيل شهادة الماجستير في علم المكتبات والعلوم الوثائقية،جامعة وهران،2014-2015 ،ص15،نقلا عن عمر أحمد همشري ،المكتبة ومهارات استخدامها،دار صفاء ، الاردن ،ص21

[13] محمود حسن الصاحب،سياسة أمن المعلومات في الجامعات حالة درسة، CYBRARIANS JOURNAL ، ع33،القاهرة ،2013، ص 2 ،متاحة على الرابط :
HTTP://JOURNAL.CYBRARIANS.ORG/INDEX.PHP?OPTION=COM_CONTENT&VIEW=ARTICLE&ID=655%3ASAHEB&CATID=265%3ARESEARCHES&ITEMID=96&FBCLID=IWAR3JCE0O1JAOH7OID0DDX4QKDCXHFGOZEAVMANBLHF_WOFBKX06FVJLNVVQ

[14] ضياء مصطفى عثمان. السرقة الالكترونية. دار النفائس. عمان. الطبعة الاولى. 2011. ص32

[15] بخي فاطمة الزهراء . اجراءات التحقيق في الجريمة الالكترونية . 2014. ص9

- ✓ **مفهوم الجريمة الالكترونية** :تعتبر الجريمة الالكترونية من الضواهر الحديثة لارتباطها بتكنولوجيا الحديثة. و لقد تعددت الجهود الرامية الى وضع تعريف محدد جامع مانع لها. حيث لم يتفق الفقه على تعريف محدد بل اذ بعض الفقهاء. ذهب الى ترجيح عدم وضع تعريف بحجة ان مثل هذا النوع من الجرائم ما هو الا جريمة تقلدية ترتكب باسلوب الكتروني [16]

مجتمع الدراسة وعينته:

- ✓ **مجتمع الدراسة:**

يعرف مجتمع البحث على أنه "كل المفردات التي يتهم الباحث بدراستها سواء كانت بشرية أو مادية بشرط اشتراكها في مجموع من الخصائص ،وتتحدد حسب طبيعة وأغراض البحث ،بهدف تعميم النتائج عليها[17]"

و في الدراسة الحالية فإن مجتمع البحث يتمثل في طلبة جامعة قاصدي مرباح ورقلة إذ تتمحور الدراسة في مجتمع فرعي ، يتمثل في طلبة قسم علوم الاعلام والاتصال وعددهم 1223.

- ✓ **عينة الدراسة:** ان اختيار العينة التي تطبق عليها الدراسة تعتبر من اهم الاعمال التي يقوم بها الباحث لانها تسهل على الباحث مشقة دراسة المجتمع الاصلي بسبب عدده وانتشاره بشرط ان تكون جزء من المجتمع الاصلي. فالعينة هي عبارة عن مجموعة من الافراد والظواهر التي تشكل المجتمع الأصلي لدراسة حيث يتم اختيارها بطريقة معينة، ومن خلالها يتم تعميم النتائج التي يتم الحصول عليها من مجتمع الدراسة الاصلي وكذلك هي اختيار جزء صغير من وحدات مجتمع البحث اختيار عشوائيا او منظما. [18]

وتعرف العينة كذلك على انها مجموعة فرعية من عناصر مجتمع البحث كما انها ذلك الجزء من المجتمع الذي يجري اختيارها وفق قواعد وطرق علمية، بحيث تمثل المجتمع تمثيلا صحيحا.[19]

ومن خلال ما سبق فقد أعتمد في الدراسة الحالية العينة الحصصية :هي تلك العينة التي تقوم على اساس تقسيم المجتمع الاصلي للبحث الى شرائح و فئات و طبقات. مهنية او اجتماعية او تعليمية...الخ . و يحدد حجم العينة على اساس ان يتناسب حجم افراد العينة المختارة مع الحجم و التعداد الاصلي لكل شريحة داخل المجتمع و نسبتها الى المجموع الكلي لمجتمع البحث [20]، لذا فان الخطوات المتبعة لاختيار عينة الدراسة كانت كما يلي :

اختيار طلبة قسم علوم الاعلام و الاتصال بجامعة قاصدي مرباح ورقلة و هذا بسبب :

---

[16] خالد ممدوح . امن الجريمة الالكترونية. الدار الجامعية. الالكترونية. الاسكندرية .2008. ص41

[17] نادية عيشور وآخرون،منهجية البحث العلمي في العلوم الاجتماعية ، مؤسسة حسين راس الجبل للنشر و التوزيع،الجزائر،2017،ص265.

[18] أحمد مرسلي، منهج البحث العلمي في علوم الاعلام والاتصال، ديوان المطبوعات الجامعية،الجزائر ، ص 183 ص 197

[19] مورس انجرس، منهجية البحث العلمي في العلوم الانسانية، ترجمة صحراوي بوزيد، ط 2، دار القصبة لنشر. الجزائر . 2004. ص301

[20] محمد سرحان علي المحمودي, مناهج البحث العلمي ,دار الكتب , صنعاء, اليمن, ط3, 2015,ص173

1. صعوبة الوصول الى جميع طلبة كلية العلوم الانسانية و الاجتماعية .لكثرة عددهم
2. الانتماء لقسم علوم الاعلام و الاتصال و هذا ما سهل علينا الدراسة الميدانية
3. بعد اختيار كلية العلوم الانسانية و الاجتماعية وقع الاختيار على قسم علوم الاعلام و الاتصال الذي قدر عدد الطلبة ب 1223 طالبا في الموسم الجامعي 2022.2023 مقسما حسب الجدول التالي :

الجدول رقم 03 : يوضح مجتمع الدراسة وحجم عينته

المستوى الجامعي	التخصص	عدد الطلبة	حجم العينة
سنة ثانية ليسانس	اعلام و اتصال	318	32
سنة ثالثة ليسانس	اتصال	298	30
سنة ثالثة ليسانس	اعلام	35	4
سنة اولى ماستر	اتصال جماهيري و الوسائط الجديدة	208	21
سنة اولى ماستر	سمعي بصري	42	5
سنة ثانية ماستر	اتصال جماهيري و الوسائط الجديدة	276	28
سنة ثانية ماستر	سمعي بصري	46	5
المجموع		1223	125

المصدر : من اعداد الطلبة

عينة الطلاب المطلوبة كانت من 127 طالباً، وسيتم تمثيلهم في العينة الحصصية على النحو التالي:

الرقم المطلوب تم اعتماده اساسا لتقسيم :

%10=125÷1223

المقاربات النظرية :

نظرية الحتمية التكنولوجية :

تعد النظرية التكنولوجية لوسائل الإعلام من النظريات الحديث التي تحدث عن دور وسائل الإعلام وطبيعة تأثيرها على مختلف المجتمعات، ويعتبر مارشال ماكلوهان من مؤسسي هذه النظرية وهو من أشهر المثقفين والباحثين في النصف الثاني من القرن العشرين. ويشكل عام يمكن القول أن هناك أسلوبان أو طريقتان للنظر إلى وسائل الإعلام:

- ✓ أنها وسائل لنشر المعلومات والترفيه والتعليم.
- ✓ أنها جزء ء من سلسلة التطور التكنولوجي.

إذا نظرنا إليها أنها وسيلة لنشر المعلومات والترفيه والتعليم، فنحن نهتم أكثر بمضمونها وطريقة استخدامها والهدف من ذلك الاستخدام وإذا نظرنا إليها كجزء من العملية التكنولوجية التي بدأت تغير وجه المجتمع كله شأنها في ذلك شأن التطورات الفنية الأخرى، فنحن نهتم حينئذ بتأثيراتها بصرف النظر عن مضمونها، يقول مارشال ماكلوهان أن مضمون وسائل الإعلام لا يمكن النظر إليه مستقلا عن تكنولوجية الوسائل الإعلامية نفسها، فالكيفية التي تعرض بها المؤسسة الإعلامية الموضوعات، والجمهور الذي توجه له رسالتها، يؤثران على ما تقوله تلك الوسائل، ولكن طبيعة وسائل الإعلام التي يتصل بها الإنسان تشكل المجتمعات أكثر مما يشكلها مضمون الاتصال، فحينما ينظر "ماكلوهان إلى التاريخ يأخذ موقفا تستطيع أن نسميه بالحتمية التكنولوجية، فبينما كان كارل ماركس يؤمن بالحتمية الاقتصادية، وبأن التنظيم الاقتصادي للمجتمع بشكل جانبا أساسيا من جوانب حتميته والمجتمع، يؤمن ماكلوهان" بأن الاختراعات التكنولوجية المهمة هي التي تؤثر تأثيرا أساسيا على المجتمعات. وقد تابع ماكلوهان" هذه الفكرة بشكل أكثر تعمنا ليعرف أهميتها التكنولوجية، مما جعله يطور فكرة محددة الصلة بين وجود الاتصال الحديث في المجتمع والتغيرات الاجتماعية التي تحدث في ذلك المجتمع، ويقول "ماكلوهان" أن التحول الأساسي في الاتصال التكنولوجي يجعل التحولات الكبرى تبدأ، ليس فقط في التنظيم الاجتماعي، ولكن أيضا في الحساسيات الإنسانية، والنظام الاجتماعي في رأيه يحدده المضمون الذي تحمله هذه عن الوسائل، وبدون فهم الأسلوب الذي تعمل بمقتضاه وسائل الإعلام لا تستطيع أن نفهم التغيرات الاجتماعية والثقافية التي تطرأ على المجتمعات.[21]

ثانيا مراحل تطور التواصل الإنساني حسب ماكلوهان:

ولأن طبيعة وسائل الإعلام المستخدمة في كل مرحلة ساعدت على تشكيل المجتمعات أكثر من المضمون، يقسم ماكلوهان بالاعتماد على وسائل الاتصال الجماهيرية، تطور التاريخ الإنساني إلى سلسلة من المراحل الثقافية والتقنية (التكنولوجية)

- ✓ المرحلة الشفوية تعتمد كلية على الاتصال الشفهي مرحلة ماقبل التعلم أو المرحلة القبلية.
- ✓ مرحلة كتابة النسخ التي ظهرت في اليونان القديمة واستمرت الفي عام الطباعة: من سنة 1500م إلى سنة 1900م تقريبا.
- ✓ عصر وسائل الإعلام الالكترونية : من سنة 1900 تقريبا على يومنا الحالي. مشيرا بذلك إلى أن التغير الأساسي في التطور الحضاري منذ أن تعلم الإنسان إن يتصل كان من الاتصال " الشفهي" إلى الاتصال " السطري" ثم إلى الاتصال الشفهي مرة أخرى.[22]

وقد قسم مراحل تطور التواصل الإنساني الى:

[21] تواتي نور الدين: "مجلة العلوم الإنسانية والاجتماعية، ماكلوهان مارشال قراءة في نظريته بين الأمس واليوم"، العدد العاشر، مارس 2013، جامعة الجزائر 3 الجزائر، ص 183

[22] بوسعيد رندا: ''التغير الاجتماعي والحتمية التكنولوجية لوسائل الإعلام، قراءة في نظرية مارشال ماكلوهان، العدد 1، 2011، جامعة الجلفة، الجزائر، ص 47

1- الاتصال الشفهي يقول ماكلوهان إن الناس يتكيفون مع الظروف المحيطة عن طريق توازن الحواس الخمس السمع البصر اللمس الشم والتذوق مع بعضها البعض، وكل اختراع جديد يعمل على تغيير التوازن بين الحواس، فقبل اختراع جوتنبرغ الحروف الكاتبة في القرن 15 كانت الثقافة السمعية هي المسيطرة وللملك تجد الشعر مثلا من أهم مظاهر التحضر حينها.[23]

2- الاتصال السطري : كانت المجتمعات في مرحلة ماقبل التعليم تحتفظ بالمضمون الثقافي في ذاكرة أجيال متعاقبة، ولكن بعدها تغير أسلوب تخزين المعرفة وأصبحت الكتب والحروف والعين مكان الأذن كوسيلة الحس الأساسية، وسمحت بتطوير المدن والهندسة والطرق البريدية والجيوش والبيروقراطية وبناء الحضارة، فالصحافة المكتوبة حسب ماكلوهان أكثر الابتكارات التكنولوجية تأثيرا على الإنسان، فالمطبوع جعله يتخلص من القبلية.

3- التواصل عن طريق المطبوع وفي اختراع جوتنبرغ الكتب والقراءة والنسخ وساعد المطبوع على نشر المصدر الفردي كوسيلة شخصية للتعامل، وأصبحت الكلمة المكتوبة أساس الحصول على المعلومة بدل الكلمة المنطوقة، وهو محور المقارنة والاختلاف بين المجمعات المتعلمة والمجتمعات ماقبل التعلم الآن التطور في نظره لم يبدأ بالثورة الصناعية في أوروبا ولكن بأول صفحة مطبوعة صحبها جوتبرغ من المطبعة.[24]

4- العودة إلى الاتصال الشفهي: يسمي ماكلوهان المرحلة التي عصر الدوائر الالكترونية وتمثل خاصة في التلفزيون الكومبيوتر ، وغيرها من الابتكارات الحديثة التي تشكل ملامح الحضارة في القرن العشرين حيث أحدثت وسائل الإعلام الالكترونية تغيرا كبيرا في توزيع الادراك الحسي او كما يسميها ماكلوهان نسبة استخدام الحواس، امتداد أي حاسة يعدل الطريقة التي تفكر أو تعمل بمقتضاها، وتعدل هذه الأخيرة الطريقة التي تدرك بها العالم وحينها تتغير تلك النسب يتغير الإنسان.

ثالثا : الوسيلة هي الرسالة: يرفض ماكلوهان نقاد وسائل الإعلام الذين يدعون أن وسائل الإعلام كتقنية حيادية وأن الاستخدام وحده من حدد قيمتها بل يدعوا إلى التفكير في طبيعة وشكل هذه الوسائل خاصة الجديدة فالتأثير العميق للسلفزيون مثلا ليس في المضمون التفافي أو السياسي بل في الطريقة التي يعمل بمقتضاها الناس الأساليب التي يستخدمون بها حواسهم وأن التكنولوجية الإعلامية أهم وألقى وأشد فعالية وأعمق تأثيرا من المضمون الفكري والسياحة اللغوية والنوايا الفردية أو الجماعية التي تصدر عنها الرسالة الإعلامية، والتلفاز مثلا كوسيلة اتصال هو بداته الرسالة وبغض النظر عن محتوى البرامج التي سوف يعرضها فإن الناس لن يتوقفوا عن مشاهدته ومما كان لفظ المشاهدة والتفاعل الذي سديه المتلقي.ويقسم ماكلوهان وسائل الإعلام في اهتمامه بتأثيراتها إلى قسمين، وسائل ساخنة ووسائل باردة حسب نمط تفاعل الأفراد معها والجهد الذي عليه فعل التلقي و المتابعة [25]

[23] نفس المرجع السابق ص 47

[24] نفس المرجع السابق ص 48

[25] نفس المرجع السابق 48

رابعا: القرية الكونية: أو القرية العالمية كما هو متواتر في الدراسات الأكاديمية تعتبر من أهم المفاهيم والعبارات الجوهرية التي طرحها مأكلوهان في نظريته والتي جاءت في كتابه " الحرب والسلم في القرية الكونية "، إذ يرى ماكلوهان أن وسائل الإعلام تحول العالم إلى قرية صغيرة عالمية، تتصل في إطارها جميع أنحاء المعمورة ببعضها البعض، في عالم يتوقف فيه الزمن وتختفي فيه المساحة فيقول إن العالم في طريقه بفضل ثورة الاتصال إلى أن يصبح قرية كونية صغيرة أو فلنقل قرية إلكترونية بشكل من الأشكال " أي أن العالم اليوم يعيش مرحلة العقل الالكتروني الموصول بشبكة من الأعصاب الممتدة إلى أجزاء الجسم الكوني، حتى إذا ما نشبت أزمة ما هنا أو حرب هناك جاءت الإشارات لتأثر في تفكير الجميع في هذا العالم وتنذرهم بالخطر المشترك، أما في وقت السلم تصبح وسائل الإعلام الالكتروني كتقنية محركا للتغير الاجتماعي

أبعاد النظرية: تبعا للنظرية، فمن الضروري جدا رسم صورة واضحة لمعرفة طبيعة عمل وسائل الإعلام كبيئة محيطة بالإنسان وكيفية تفاعله مع كل نوع من أنواع وسائل الإعلام، وغياب هذه الصورة سوف يكون مستحيلا فهم العلاقة بين التطور الثقافي والإجتماعي المحيط بوسائل الإعلام ولكن المشكلة هي أن تحليل بيئة وسائل الإعلام عملية صعبة جدا، لأن كل نوع من أنواع وسائل الإعلام يخلق بيئة مختلفة وجميع هذه البيئات غير ملموسة ومتداخلة مع بعضها البعض. فالبيئة التي تخلقها الرسائل القصيرة بنقل الأخبار كالواتساب هي مختلفة عن متابعة الأخبار عن طريق الشبكة الإجتماعية كتويتر، ولكنه في النهاية هي متشابكة مع بعضها لأن تعامل الإنسان يكون معهما على حد سواء، يصبح الفصل بينهما كبيئتين مختلفتين أمر بحاجة لآلاف الساعات من المراقبة والتحليل ليتم فهم كيف يعمل هذا النوع من الإعلام على الأفراد وكيف ينمط حياتهم، يقول ماكلومان إن الوسيط يغيرنا ويؤثر على البنية الفردية والإجتماعية، لأنها نتفاعل معه مرارا وتكرارا حتى يصبح جزءا من انفسنا، فنحن اليوم لا نستطيع تخيل حياتنا بلا الهواتف الذكية والإنترنت لأن كل وسيط بدفعنا لإستخدام حواس معينة ليخلق عادة تداوم على ممارستها إن الإنخراط يشكل يومي في أحد الوسائط يوما بعد يوم يحضر أحد الحواس لدينا لاستخدامها أكثر من غيرها، فالوسيعة السمعي كالاغاني مثلا يحفز حاسة السمع أكثر من حاسة النظر إذا تم إستخدامها بشكل أكبر، وعلى الصعيد الإجتماعي المجتمع يصالح بحسب الوسيط الأكثر إنتشارا بين أفراده .[26]

عندما تدخل تكنولوجيا إعلامية جديدة يمر المجتمع فترة تصبح هذه التكنولوجيا ظاهرة غريبة يتحدث الجميع عنها، في هذه المرحلة يبدأ الأفراد تعلم هذه الوسيلة. وفي المرحلة الثانية عندما تصبح هذه التكنولوجيا في متناول أيدي الجميع تصبح ظاهرة إعتيادية وتختفي في خلفية عادات المجتمع وعندها ينخرط الأفراد تحت الأنماط البيئية التي يخلقها هذا النوع من الإعلام وتصبح جزء أساسي من تكوينه، وكأبسط مثال فكر في دخول الهواتف الذكية لحياتنا وما العادات الجديدة التي اكتسبناها بسببه . ويكون الإنخراط في هذه البيئة التكنولوجية للأفراد الذين نشؤوا مع هذه التكنولوجيا كالأطفال الذين بدؤوا طفولتهم بالرسم على ال padi أكبر من الذين شهدوا دخول هذه التكنولوجيا وحاولوا تعلمها. فالأجيال التي تكبر بوجود هذه التكنولوجيا لن يستطيعوا أبدا تخيل العالم بدونها ليس كمن شهدو اختراعها.[27]

[26] عبد الرزاق الدليمي: ''نظريات الاتصال في القرن الحادي والعشرين "، دار اليازوري العلمية، ط1، عمان، الأردن، 2016، ص 299

[27] نفس المرجع السابق ص 299

إسقاط النظرية على الدراسة الحالية : بإسقاط هذه النظرية على الدراسة الحالية ،نجد أنه نتيجة للتطورات في التكنولوجيات ،أصبح الطلبة يتلقون المعلومات الأمنية في مجال تكنولوجيا الاتصال والمعلومات ،فتعد هذه الوسائل امتدادا لحواسهم ، وأن الوسيلة التي يتم بها عرض المعلومات المتعلقة بالأمن المعلوماتي تؤثر في المضمون الذي تبثه إلى الطلبة ،وهناك وسائل اتصال مختلفة (ساخنة وباردة) تهتم بنقل المضامين المتعلقة بالأمن المعلوماتي للطلبة، و تؤثر التطورات التكنولوجية تأثيرا حتميا على الطلبة وذلك من خلال تكيفهم مع طرق الحماية المتاحة وغيرها من المستجدات وأيضا اكتساب ثقافة نسبية قد تختلف باختلاف الجنس والمستوى التعليمي .

الجانب التطبيقي

تمهيد:

يتناول هذا الإطار التحليل بيانات الدراسة الميدانية استنادا للمعطيات المتحصل عليها من استمارات الاستبيان التي تم توزيعها على المبحوثين والتي قدرت ب 125 مفردا حيث تم استرجاع جميعها وبعد عمليه الترقيم الاستمارات من واحد الى 125 وترميزها وفقا نظام spss قمنا بتفريغها وادخال البيانات في الحاسوب وقد تم وضع الإجابات في شكل جداول تحمل تكرارات ونسب مئوية مع التعليق عليها كما وكيفيا وايجاد نتائج تفسيرات ذات دلالات لأجوبة الطلبة المبحوثين.

البيانات الشخصية لأفراد العينة:

تساعد البيانات الشخصية الباحث في التعرف على ملامح وخصائص أفراد العينة كما يعتمد عليها الباحث كمؤشرات في تحليل البيانات الميدانية وفق ما يراه وتقتضيه متغيرات الدراسة واهدافها لذلك اشتملت دراستنا على معرفة البيانات الشخصية لأفراد العينة وتضمنت اربعة أسئلة الجنس، السن .المستوى الجامعي. التخصص.

نتائج المحور الأول: المصادر المسؤلة عن تشكيل ثقافة امن المعلوماتي لدى الطلبة الجامعيين.

نتائج المحور الثاني: مدى اطلاع الطالب على اساليب و طرق الاختراق الالكتروني.

نتائج المحور الثالث: معرفة الطالب بكيفية حماية بياناته على مواقع الويب المختلفة.

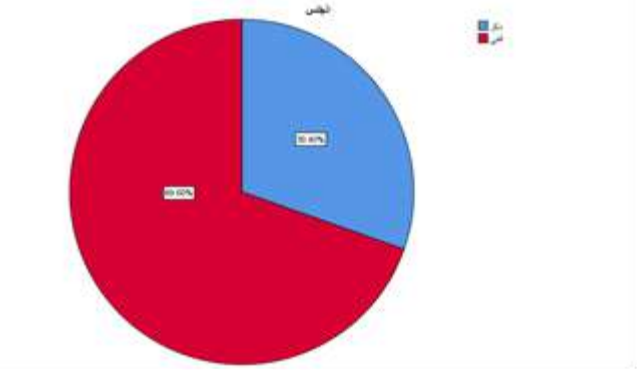
عرض و تحليل نتائج الاستبيان:

الجدول رقم 04 : يوضح توزيع افراد العينة حسب الجنس

الجنس	التكرار	النسبة المئوية
ذكر	38	30.4
انثى	87	69.6
المجموع	125	100.0

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

الشكل رقم 01 : يوضح توزيع افراد العينة حسب الجنس



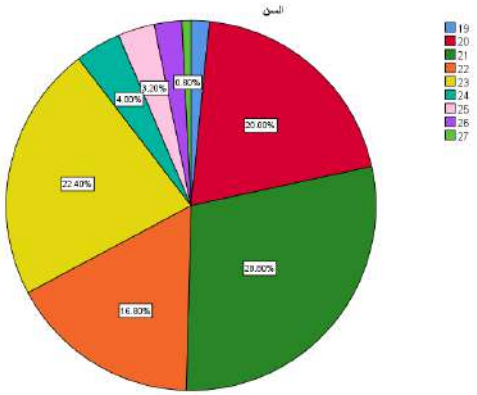
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

يتضح من خلال الجدول 04 ان توزيع افراد العينة حسب متغير الجنس يتكون من 87 انثى و 38 كر و قد كانت نسبة الاناث هي النسبة الاكبر مقارنة با الذكور فمن خلال النتائج المبينة في الجدول يتضح ان الاناث لهم اهتمام أكبر بمجال أمن المعلومات وبالتالي يكون لديهن دافع أكبر للتعرف عليه

الجدول رقم 05 : يوضح توزيع افراد العينة حسب السن

السن	التكرار	النسبة المئوية
19	2	1.6
20	25	20.0
21	36	28.8
22	21	16.8
23	28	22.4
24	5	4.0
25	4	3.2
26	3	2.4
27	1	8.
المجموع	125	100.0

الشكل رقم 02 : يوضح توزيع افراد العينة حسب السن



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

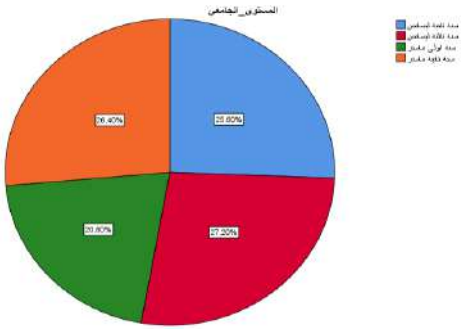
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

يوضح الجدول رقم 05 توزيع العينة حسب متغير السن حيث نجد أن النسبة الكبيرة في العمر هي 21 سنة وقد قدرت بنسبة 28.8 بالمئة وبعدها نجد 23 سنة بنسبة 22.4 بالمئة وبعدها سن 20 بنسبة 20 بالمئة ثم 22 سنة بنسبة 16.8 بالمئة و اخيرا سن 26 بنسبة 2.4بالمئة. يبين الجدول ان العمر 21 سنة هم الذين لهم اهتمام أكبر بمجال أمن المعلومات ذلك لاستخدامهم الاجهزة التكنولولوجيا بدرجة كبيرة

الجدول رقم 06 : يوضح توزيع افراد العينة حسب المستوى التعليمي

المستوى التعليمي	التكرار	النسبة المئوية
سنة ثانية ليسانس	32	25.6
سنة ثالثة ليسانس	34	27.2
سنة اولى ماستر	26	20.8
سنة ثانية ماستر	33	26.4
المجموع	125	100.0

الشكل رقم 03 : يوضح توزيع افراد العينة حسب المستوى التعليمي



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

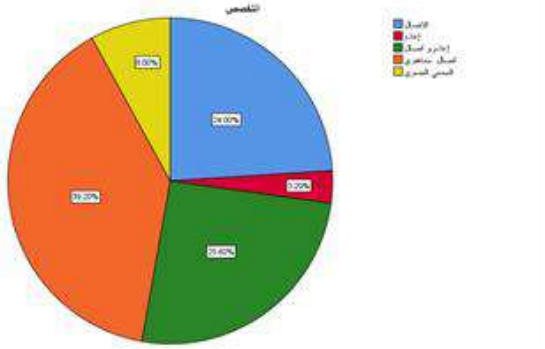
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

يوضح الجدول رقم 6 توزيع العينة حسب متغير المستوى في قسم علوم الأعلام و الاتصال الذي تم توزيع استمارة الاستبيان عليه حيث نجد ان الفئة الاكبر في سنة ثالثة ليسانس بنسبة 27.2 وبعدها السنة ثانية ماستر بنسبة 26.4 ثم تليها سنة سنة ثانية ليسانس بنسبة 25.6 بالمئة وفي الاخير السنة اولى ماستر 20.8 بالمئة وقد كان توزيعنا لمعينة عشوائي

الجدول رقم 07 : يوضح توزيع افراد العينة حسب التخصص الجامعي

الشكل رقم 04 : يوضح توزيع افراد العينة حسب التخصص الجامعي

التخصص الجامعي	التكرار	النسبة المئوية
الاتصال	30	24.0
إعلام	4	3.2
إعلام و اتصال	32	25.6
اتصال جماهيري	49	39.2
السمعي البصري	10	8.0
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

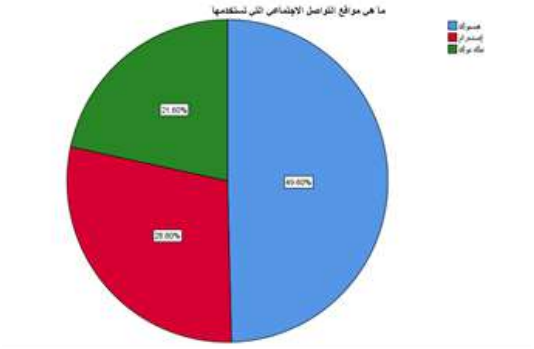
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

يوضح الجدول رقم 7 توزيع العينة حسب متغير التخصص في قسم علوم الاعلام و الاتصال حيث نجد ان الفئة الاكبر في تخصص اتصال جماهيري بنسبة 39.2 وبعدها تخصص إعلام و اتصال بنسبة 25.6 ثم يليها تخصص الاتصال بنسبة 24ثم تخصص السمعي البصري بنسبة 8 بالمئة وفي الاخير تخصص اعلام 3.2 بالمئة وقد كان توزيعنا لمعينة عشوائي

الفئات	التكرار	النسبة المئوية
فيسبوك	62	49.6
إنستغرام	36	28.8
تيك توك	27	21.6
المجموع	125	100.0

الجدول رقم 08 : يوضح مواقع التواصل المستخدمة

الشكل رقم 05 : يوضح مواقع التواصل المستخدمة



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

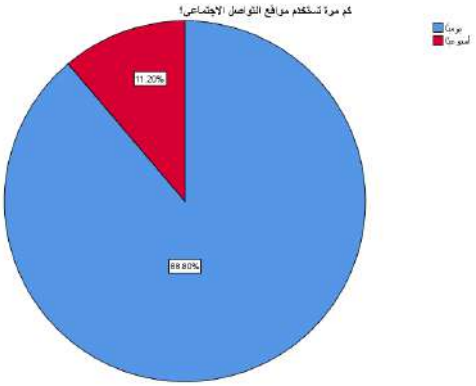
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تفضيل استخدام مواقع التواصل الاجتماعي حيث احتل فيها "الفيسبوك" النسبة الأكبر حيث بلغت هذه النسبة 49.6%بينما قدرت نسبة "انستقرام" 28.8%يليها "التيكتوك" البالغة نسبتهم .21.6%
نستخلص من ذلك أن الفيسبوك يعد من أهم مواقع التواصل المستخدمة و يعود ذلك إلى تنوع المحتوى حيث يوفر فيسبوك محتوى متنوعًا يشمل الصور والفيديوهات والمقالات والأخبار والمناسبات والفعاليات

الجدول رقم 09 : يوضح مرات استخدام مواقع التواصل الاجتماعي

الفئات	التكرار	النسبة المئوية
يوميًا	**111**	**88.8**
أسبوعيًا	**14**	**11.2**
المجموع	**125**	**100.0**

الشكل رقم 06 : يوضح مرات استخدام مواقع التواصل الاجتماعي



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

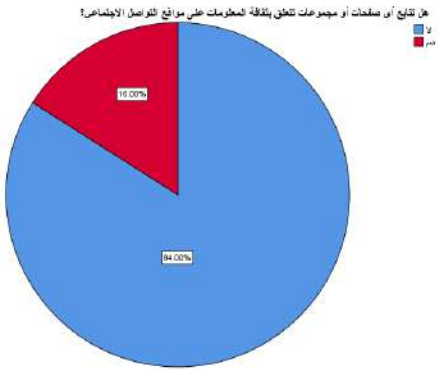
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب مرات استخدام مواقع التواصل الاجتماعي إلى ثلاث فئات رئيسية احتل فيها "يوميا" النسبة الأكبر حيث بلغت هذه النسبة 88.8%بينما قدرت نسبة "أسبوعيًا"11.2%يليها "شهريا" البالغة نسبتهم . 0

نستخلص من ذلك أن غالبية المبحوثين يتصفحون يوميا مواقع التواصل الاجتماعي وقد يعود السبب في ذلك إلى الاهتمام الكبير بهذه المواقع

الجدول رقم 10: يوضح متابعة صفحات تتعلق بثقافة المعلومات على التواصل الاجتماعي

الفئات	التكرار	النسبة المئوية
لا	105	84.0
نعم	20	16.0
المجموع	125	100.0

الشكل رقم 07 : يوضح متابعة صفحات تتعلق بثقافة المعلومات على التواصل الاجتماعي



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

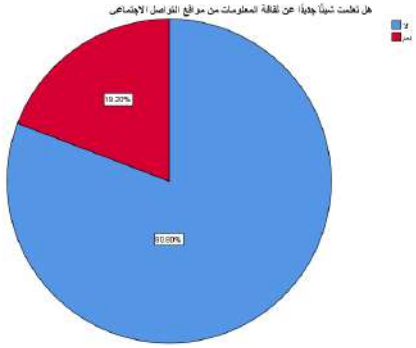
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب متابعة أي صفحات أو مجموعات تتعلق بثقافة المعلومات على مواقع التواصل الاجتماعي حيث اغلبية المبحوثين جابوا با لا و بلغت هذه النسبة 84% بينما الين اجابوا با لا بلغت نسبتهم 16 نستخلص من ذلك أن الاغلبية يعتبر مواقع التواصل الاجتماعي تستخدم للتواصل مع الأصدقاء والعائلة والاستمتاع بالوقت، وليس للتعلم و متابعة الصفحات التي تتعلق با ثقافة امن المعلومات

الجدول رقم 11 :تعلم شيئ جديد عن ثقافة المعلومات من مواقع التواصل الاجتماعي

الفئات	التكرار	النسبة المئوية
لا	101	80.8
نعم	24	19.2

الشكل رقم 08 : تعلم شيئ جديد عن ثقافة المعلومات من مواقع التواصل الاجتماعي

المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

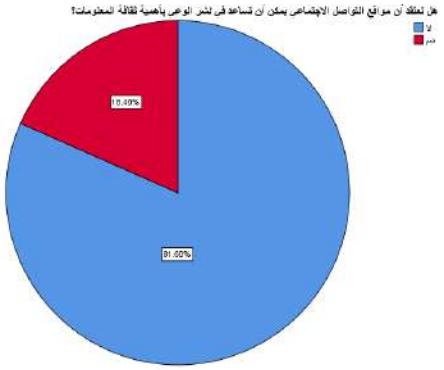
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تعلم شيئًا جديدًا عن ثقافة المعلومات من مواقع التواصل الاجتماعي حيث اغلبية المبحوثين اجابوا ب لا و بلغت هذه النسبة 80.8%بينما الين اجابوا با نعم بلغت نسبتهم 19.2 نستخلص من ذلك أن الاغلبية غير مهتمين بثقافة امن المعلومات ولا يرونها كموضوع هام يستحق الاهتمام

الجدول رقم 12 :نشر الوعي باهمية ثقافة المعلومات على مواقع التواصل الاجتماعي

الفئات	التكرار	النسبة المئوية
لا	102	81.6
نعم	23	18.4
المجموع	125	100.0

الشكل رقم 09 : نشر الوعي باهمية ثقافة المعلومات على مواقع التواصل الاجتماعي



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

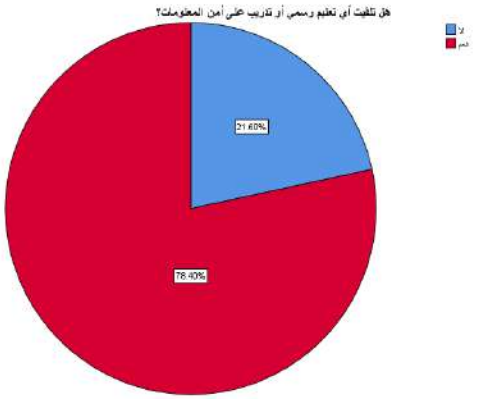
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الاعتقاد أن مواقع التواصل الاجتماعي يمكن أن تساعد في نشر الوعي بأهمية ثقافة امن المعلومات حيث اغلبية المبحوثين اجابوا بلا و بلغت هذه النسبة 81.6%بينما الذين اجابوا با نعم بلغت نسبتهم 18.4 نستخلص من ذلك أن الاغلبية لا يرى ان مواقع التواصل الاجتماعي تساعد في نشر الوعي باهمية ثقافة امن المعلومات لقصر الرسائل والمنشورات على مواقع التواصل الاجتماعي و هذا غير كافي لتوضيح أهمية ثقافة أمن المعلومات وكيفية الحفاظ على الخصوصية والأمان عبر الإنترنت.

الجدول رقم 13 :تلقي التعليم على امن المعلومات

الشكل رقم 10 : تلقي التعليم على امن المعلومات

الفئات	التكرار	النسبة المئوية
لا	27	21.6
نعم	98	78.4
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

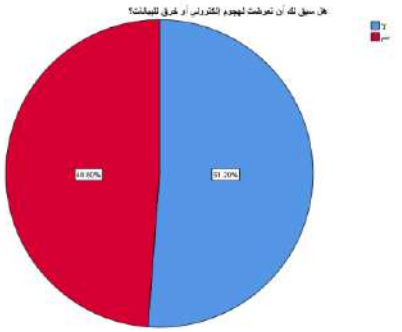
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تلقي أي تعليم رسمي أو تدريب على أمن المعلومات حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 78.4 % بينما الذين اجابوا با نعم بلغت نسبتهم 21.6 نستخلص من ذلك أن الاغلبية تلقوا تعليم رسمي أو تدريب على أمن المعلومات ذلك لأنه يعتبر أحد التحديات الكبيرة التي تواجهها المؤسسات والأفراد في العصر الرقمي الحالي. فمع التطور الكبير لتقنيات الحاسوب وشبكات الإنترنت، أصبح من الضروري حماية المعلومات الحساسة التي يتم تبادلها عبر الإنترنت من الاختراقات والهجمات الإلكتروني

الجدول رقم 14 :تعرض لهجوم الكتروني او خرق للبيانات

الشكل رقم 11 : تعرض لهجوم الكتروني او خرق للبيانات

الفئات	التكرار	النسبة المئوية
لا	64	51.2
نعم	61	48.8
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

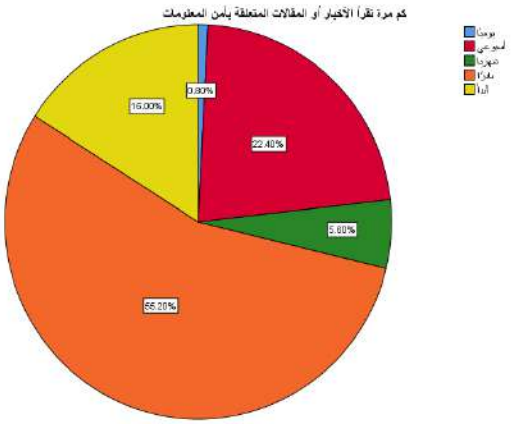
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب التعرض لهجوم إلكتروني أو خرق للبيانات حيث هناك تقارب بين المبحوثين فا الذين جابوا با لا بلغت نسبتهم 51.2% بينما الذين اجابوا با نعم بلغت نسبتهم 48.2 نستخلص من ذلك أن الأفراد الذين لم يتعرضوا للاختراق قد اتبعوا الممارسات الأمنية السليمة، مثل استخدام كلمات مرور قوية وتحديث البرامج والتطبيقات بانتظام، فقد يكونون أكثر حماية من الأفراد الذين لم يتبعوا هذه الممارسات وتعرضوا للاختراق.

الجدول رقم 15 :عدد قراءة الأخبار أو المقالات المتعلقة بأمن المعلومات

الفئات	التكرار	النسبة المئوية
يوميًا	1	8.
أسبوعي	28	22.4
شهريا	7	5.6
نادرًا	69	55.2
أبداً	20	16.0
المجموع	125	100.0

الشكل رقم 12 : عدد قراءة الأخبار أو المقالات المتعلقة بأمن المعلومات



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

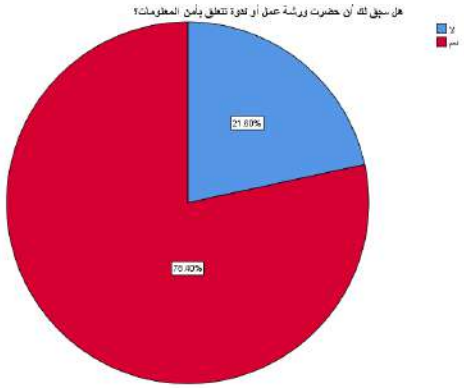
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب قراءة الأخبار أو المقالات المتعلقة بأمن المعلومات حيث كانت الاجابة " نادرًا " النسبة الأكبر حيث بلغت هذه النسبة 55.2 % بينما قدرت نسبة " أسبوعيا" 22.4% يليها " أبداً " البالغة نسبتهم .% 16.0 ثم " شهريا" بنسبة 5.6% و اخيرا يوميا با نسبة 0.8 نستخلص من ذلك أن نادرا ما يقرؤن الأخبار أو المقالات المتعلقة بأمن المعلومات و ذلك لعدم الادراك باهمية أمن المعلومات وخطورة التهديدات التي قد تواجههم، مما يؤدي إلى عدم اهتمامهم بالموضوع

الجدول رقم 16 :عدد حضور ورشات العمل او ندوة تتعلق بأمن المعلومات

الفئات	التكرار	النسبة المئوية
لا	27	21.6
نعم	98	78.4
المجموع	125	100.0

الشكل رقم 13 : عدد حضور ورشات العمل او ندوة تتعلق بأمن المعلومات



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

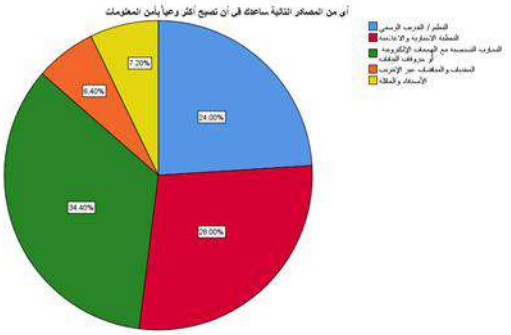
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب حضور ورشة عمل أو ندوة تتعلق بأمن المعلومات حيث اغلبية المبحوثين اجابوا بنعم و بلغت هذه النسبة 78.4%بينما الذين اجابوا با لا بلغت نسبتهم 21.6 نستخلص من ذلك أن الاغلبية حضروا ورشة عمل أو ندوة تتعلق بأمن المعلومات لحصول على معلومات قيّمة عن كيفية حماية بياناتهم الشخصية والمعلومات المهنية من الاختراق والاستغلال غير المصرح به

الجدول رقم 17 :المصادر التي تساعد على الوعي بأمن المعلومات

الفئات	التكرار	النسبة المئوية
التعليم / التدريب الرسمي	30	24.0
التغطية الاخبارية والاعلامية	35	28.0
التجارب الشخصية مع الهجمات الإلكترونية أو خروقات البيانات	43	34.4
المنتديات والمناقشات عبر الإنترنت	8	6.4
الأصدقاء والعائلة	9	7.2
المجموع	125	100.0

الشكل رقم 14 : المصادر التي تساعد على الوعي بأمن المعلومات



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

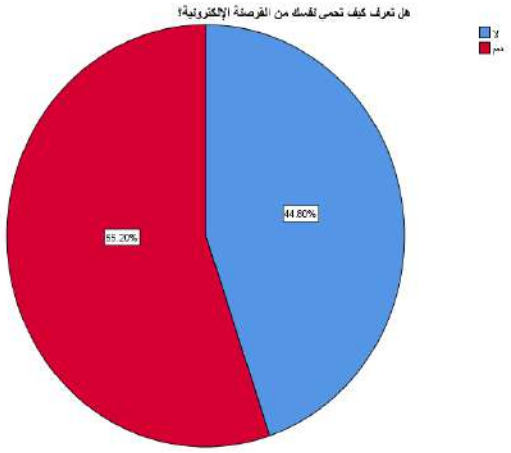
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب المصادر المساعدة في زيادة الوعي بأمن المعلومات حيث احتل فيها "التجارب الشخصية مع الهجمات الإلكترونية أو خروقات البيانات" النسبة الأكبر حيث بلغت هذه النسبة 34.4%بينما قدرت نسبة "التغطية الاخبارية والاعلامية" 28%يليها "التعليم / التدريب الرسمي" البالغة نسبتهم .24% ثم "الأصدقاء والعائلة" با نسبة 7.2 و اخيرا "المنتديات والمناقشات عبر الإنترنت" البالغة نسبتهم 6.4 نستخلص من ذلك أن التجارب الشخصية مع الهجمات الإلكترونية أو خروقات البيانات تعد من أهم المصادر المساعدة في زيادة الوعي بأمن المعلومات و يعود ذلك لان العديد من الأفراد قد يكونون غير عائِزين عن أهمية حماية معلوماتهم الشخصية والبيانات الحساسة، حتى يتعرضوا لهجوم إلكتروني أو خرق للبيانات. وبعد تجربة هذه الأمور بأنفسهم، يصبحون أكثر وعيًا بالتحديات التي يواجهونها في هذا الصدد، ويتعلمون كيفية الوقاية منها والتصرف بطريقة صحيحة عند حدوثها. وبالتالي، فإن هذه التجارب تسهم في رفع مستوى الوعي بأهمية الأمن السيبراني والحاجة إلى اتباع ممارسات التأمين السليمة لحماية المعلومات الحساسة والبيانات الشخصية.

الجدول رقم 17 :معرفة كيفية حماية النفس من القرصنة الالكترونية

الشكل رقم 14 : معرفة كيفية حماية النفس من القرصنة الالكترونية

الفئات	التكرار	النسبة المئوية
لا	56	44.8
نعم	69	55.2
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

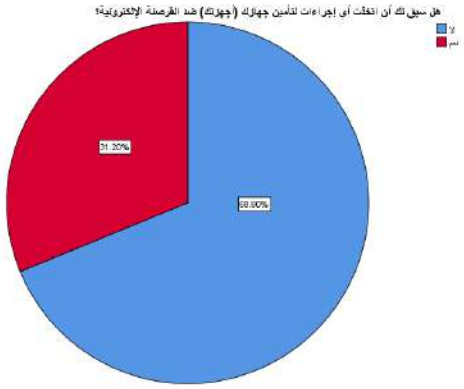
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب المعرفة حول تعرف كيفية حماية انفسهم من القرصنة الإلكترونية حيث اجابات المبحوثين كانت متقاربة فا الذين جابوا با نعم بلغت نسبتهم 55.2% بينما الذين اجابوا با لا بلغت نسبتهم 44.8 نستخلص من ذلك أن الأشخاص الذين يعرفون كيفية حماية أنفسهم من القرصنة الإلكترونية يقوم بالاطلاع على آخر التطورات الأمنية والحفاظ على التوعية الأمنية، وذلك من خلال متابعة المصادر الموثوقة والمتخصصة في هذا المجال.

الجدول رقم 18 :إجراءات تامين من القرصنة الالكترونية

الفئات	التكرار	النسبة المئوية
لا	86	68.8
نعم	39	31.2
المجموع	125	100.0

الشكل رقم 15 : اجراءات تامين من القرصنة الالكترونية



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

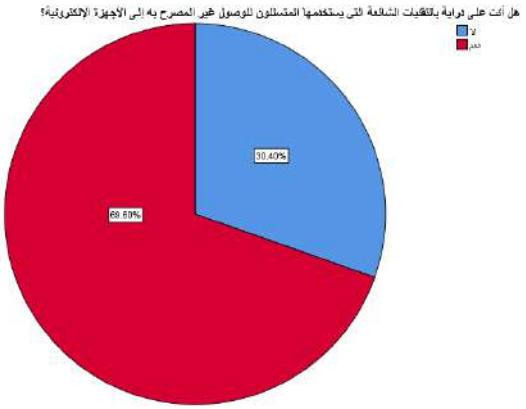
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب اتخاذ أي إجراءات لتأمين أجهزتهم ضد القرصنة الإلكترونية حيث اغلبية المبحوثين اجابوا بلا و بلغت هذه النسبة 68.8%بينما الذين اجابوا با نعم بلغت نسبتهم 31.2 نستخلص من ذلك أن الاغلبية لا يتخذون أي إجراءات لتأمين أجهزتهم ضد القرصنة الإلكترونية للاعتقاد بأنهم غير مستهدفين من القرصنة الإلكترونية، وبالتالي فإنهم لا يرون الحاجة إلى اتخاذ إجراءات لحماية أجهزتهم

الجدول رقم 19 :الدراية بالتقنيات للتسلل الى الاجهزة الالكترونية

الفئات	التكرار	النسبة المئوية
لا	38	30.4
نعم	87	69.6
المجموع	125	100.0

الشكل رقم 16 : الدراية بالتقنيات للتسلل الى الاجهزة الالكترونية



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

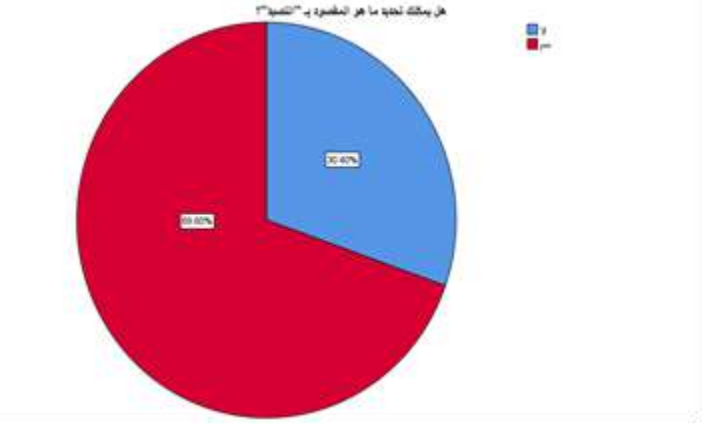
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الدراية بالتقنيات الشائعة التي يستخدمها المتسللون للوصول غير المصرح به إلى الأجهزة الإلكترونية حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 69.6%بينما الذين اجابوا با لا بلغت نسبتهم 30.4

نستخلص من ذلك أن الاغلبية لهم دراية بالتقنيات الشائعة التي يستخدمها المتسللون للوصول غير المصرح به إلى الأجهزة الإلكترونية ذلك لكون انهم لديهم تجارب سابقة مع الاختراق السيبراني، سواء بسبب جهاز كمبيوتر شخصي أو هاتف ذكي تعرض للاختراق. هذه التجارب قد تدفعهم لتعلم كيفية الحماية واتخاذ الإجراءات اللازمة لتجنب تكرار هذه التجربة المؤلمة.

الجدول رقم 20 :تحديد المقصود بالتصيد

الفئات	التكرار	النسبة المئوية
لا	38	30.4
نعم	87	69.6
المجموع	125	100.0

الشكل رقم 17: تحديد المقصود بالتصيد



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تحديد ما هو المقصود بـ "التصيد"حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 69.6%بينما الذين اجابوا با لا بلغت نسبتهم 30.4

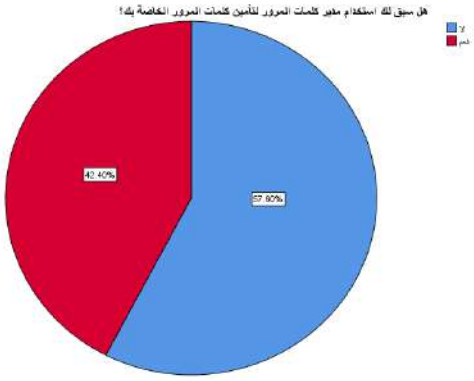
نستخلص من ذلك أن الاغلبية يعلم با ما هو المقصود بـ "التصيد" ذذلك لكونهم يتلقون حملات توعوية تحذرهم من خطر البريد الإلكتروني المزيف وغيرها من التهديدات الأمنية على الإنترنت

الجدول رقم 21 :استخدام المدير كلمات المرور الخاصة

الفئات	التكرار	النسبة المئوية
لا	72	57.6
نعم	53	42.4
المجموع	125	100.0

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

الشكل رقم 18 : استخدام المدير كلمات المرور الخاصة



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

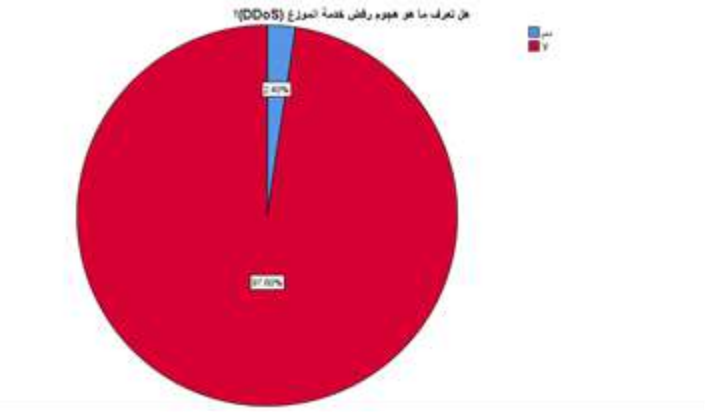
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب استخدام مدير كلمات المرور لتأمين كلمات المرور الخاصة بهم حيث اغلبية المبحوثين اجابوا بلا و بلغت هذه النسبة 57.6%بينما الذين اجابوا با نعم بلغت نسبتهم 42.4

نستخلص من ذلك أن الاغلبية لا يستخدم مدير كلمات المرور لتأمين كلمات المرور الخاصة بهم ذلك لانهم قد يشعرون بالملل من استخدام مدير كلمات المرور ويفضلون استخدام كلمات المرور القصيرة والسهلة التذكر

الجدول رقم 22 :معرفة هجوم رفض خدمة الموزع

الشكل رقم 19 : معرفة هجوم رفض خدمة الموزع

الفئات	التكرار	النسبة المئوية
لا	3	2.4
نعم	122	97.6
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

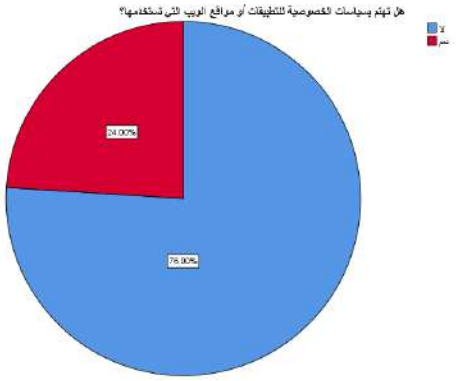
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب معرفة هجوم رفض خدمة الموزع (DDoS) حيث اغلبية المبحوثين اجابوا بلا و بلغت هذه النسبة 97.6%بينما الذين اجابوا بنعم بلغت نسبتهم 2.4 نستخلص من ذلك أن الاغلبية لا يعرف هجوم رفض خدمة الموزع (DDoS) لقلة الوعي التقني حيث يعتبر هجوم رفض خدمة الموزع من التهديدات الأمنية التي تحتاج إلى فهم تقني متطور، مما يجعلها صعبة بالنسبة للأشخاص غير الملمين بالأمن المعلوماتي.

الجدول رقم 23 :الاهتمام بسياسات الخصوصة للتطبيقات او مواقع الويب المستخدمة

الفئات	التكرار	النسبة المئوية
لا	95	76.0
نعم	30	24.0
المجموع	125	100.0

الشكل رقم 20 : الاهتمام بسياسات الخصوصة للتطبيقات او مواقع الويب المستخدمة



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

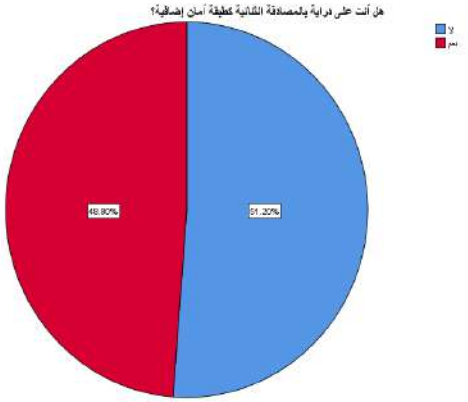
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الاهتمام بسياسات الخصوصية للتطبيقات أو مواقع الويب التي يستخدمها حيث اغلبية المبحوثين جابوا با لا و بلغت هذه النسبة 76.0%بينما الذين اجابوا با نعم بلغت نسبتهم 24.0

نستخلص من ذلك أن الاغلبية لا يهتم بسياسات الخصوصية للتطبيقات أو مواقع الويب التي يستخدمها لعدم رؤية المخاطر حيث لا يدركون المخاطر المحتملة لعدم الاهتمام بسياسات الخصوصية، والتي يمكن أن تتضمن جمع البيانات الشخصية ومشاركتها مع أطراف ثالثة دون علم المستخدمين.

الجدول رقم 24 :الدراية بالمصادقة الثنائية كطبقة امان

الفئات	التكرار	النسبة المئوية
لا	64	51.2
نعم	61	48.8
المجموع	125	100.0

الشكل رقم 21 : الدراية بالمصادقة الثنائية كطبقة امان



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

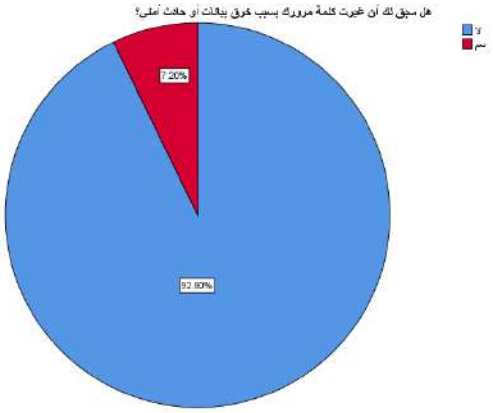
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الدراية بالمصادقة الثنائية كطبقة أمان إضافية حيث نرى اغلبية اجابات المبحوثين اجابوا بلا بلغت نسبتهم 51.2 % بينما الذين اجابوا بنعم بلغت نسبتهم 48.8 نستخلص من ذلك أن قد يكون لديهم فهم ضعيف للتقنية والأمان الإلكتروني، مما يجعلهم غير ملمين بأهمية المصادقة الثنائية.

الجدول رقم 25 :تغيير كلمة المرور بسيت خرق بيانات او حادث امني

الفئات	التكرار	النسبة المئوية
لا	116	92.8
نعم	9	7.2
المجموع	125	100.0

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

الشكل رقم 22 : تغيير كلمة المرور بسيت خرق بيانات او حادث امني



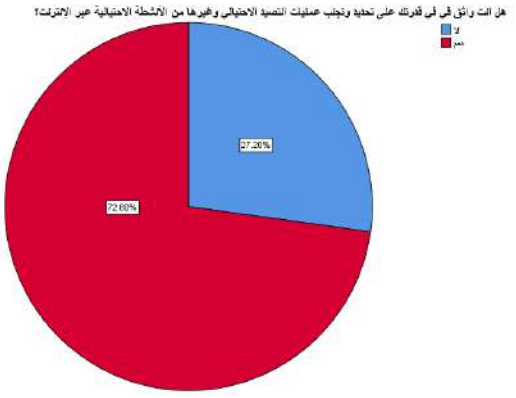
المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تغيير كلمة المرور بسبب خرق بيانات أو حادث أمني حيث اغلبية المبحوثين جابوا با لا و بلغت هذه النسبة 92.8% بينما الذين اجابوا با نعم بلغت نسبتهم 7.2

نستخلص من ذلك أن الاغلبية لم يغيير كلمة المرور بسبب خرق بيانات أو حادث أمني للإهمال حيث يتجاهلون أهمية تغيير كلمات المرور بعد وقوع خرق بيانات أو حادث أمني، يتجاهلون ذلك أو يؤجلونه إلى وقت لاحق.

الجدول رقم 26 :الوثوق في القدرات و تجنب عمليات التصيد الشكل رقم 23 : الوثوق في القدرات و تجنب عمليات التصيد

الفئات	التكرار	النسبة المئوية
لا	34	27.2
نعم	91	72.8
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

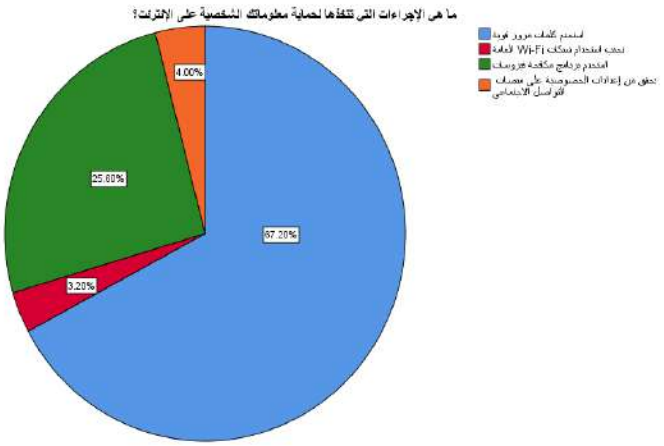
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الوثوق في القدرة على تحديد وتجنب عمليات التصيد الاحتيالي وغيرها من الأنشطة الاحتيالية عبر الإنترنت حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 72.8%بينما الذين اجابوا بلا بلغت نسبتهم 27.2 نستخلص من ذلك أن الاغلبية واثق في القدرة على تحديد وتجنب عمليات التصيد الاحتيالي وغيرها من الأنشطة الاحتيالية عبر الإنترنت و يرجع ذلك لثقة الزائدة حيث يمكنهم الاعتماد بشكل زائد على خدمات الحماية الإلكترونية مثل برامج مكافحة الفيروسات والجدران النارية، مما يجعلهم يشعرون بالثقة الكبيرة في قدرتها على حماية اجهزتهم والبيانات الشخصية.

الجدول رقم 27 :الاجراءات المتخذة لحماية المعلومات الشخصية

الفئات	التكرار	النسبة المئوية
استخدم كلمات مرور قوية	84	67.2
تجنب استخدام شبكات Wi-Fi العامة	4	3.2

الشكل رقم 24 : الاجراءات المتخذة لحماية المعلومات الشخصية

استخدم برنامج مكافحة فيروسات	32	25.6
تحقق من إعدادات الخصوصية على منصات التواصل الاجتماعي	5	4.0
المجموع	**125**	**100.0**



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الإجراءات المتخذة لحماية معلوماتهم الشخصية على الإنترنت حيث اغلبية المبحوثين جابوا با استخدم كلمات مرور قوية و بلغت هذه النسبة 67.2% ثم تليها الذين اجابوا استخدم برنامج مكافحة فيروسات با نسبة 25.6 بينما الذين اجابوا با تحقق من إعدادات الخصوصية على منصات التواصل الاجتماعي بلغت نسبتهم 4.0 و خيرا بلغت نسبة الذين اجابوا با تجنب استخدام شبكات Wi-Fi العامة ب 3.2 نستخلص من ذلك أن الاغلبية يستخدمون كلمات مرور قوية للحماية معلوماتهم الشخصية على الإنترنت لزيادة الوعي حيث يزداد الوعي بأهمية استخدام كلمات مرور قوية

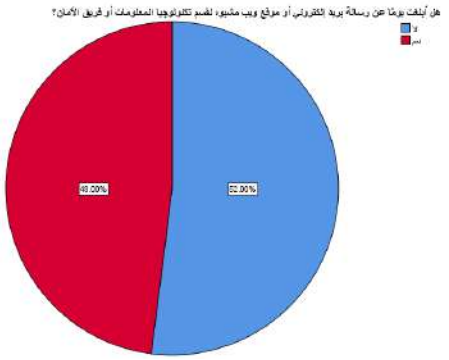
لحماية المعلومات الشخصية على الإنترنت، و يتم توعية المستخدمين بشكل مستمر من خلال حملات الإعلام والإعلانات والنصائح الأمنية.

الجدول رقم 28 :الابلاغ عن رسالة بريد الكتروني او موقع مشبوه لقسم تكنولوجيا المعلومات أو فريق الأمان

الفئات	التكرار	النسبة المئوية
لا	65	52.0
نعم	60	48.0
المجموع	**125**	**100.0**

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

الشكل رقم 25 : الابلاغ عن رسالة بريد الكتروني او موقع مشبوه لقسم تكنولوجيا المعلومات أو فريق الأمان



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الابلاغ عن رسالة بريد إلكتروني أو موقع ويب مشبوه لقسم تكنولوجيا المعلومات أو فريق الأمان حيث اغلبية المبحوثين اجابوا با لا و بلغت هذه النسبة 52%بينما الذين اجابوا با نعم بلغت نسبتهم 48

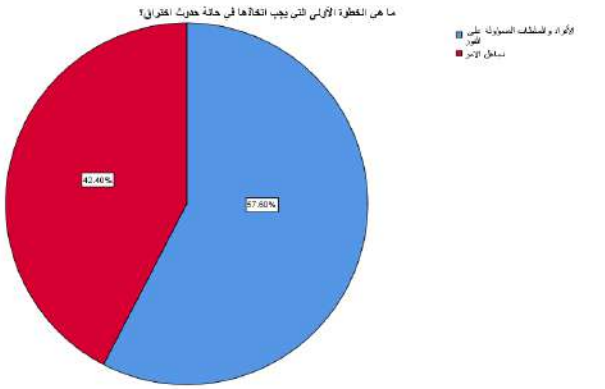
نستخلص من ذلك أن الاغلبية لا يبلغون عن رسالة بريد إلكتروني أو موقع ويب مشبوه لقسم تكنولوجيا المعلومات أو فريق الأمان لجهلهم خطورة هذه الرسائل الإلكترونية أو المواقع المشبوهة، ولا يدركون ما هي التدابير الأمنية التي يجب اتخاذها لحماية أنفسهم

الجدول رقم 29 : الخطوة الأولى التي يجب اتخاذها في حالة حدوث اختراق

الفئات	التكرار	النسبة المئوية

الشكل رقم 26 : الخطوة الأولى التي يجب اتخاذها في حالة حدوث اختراق

إخطار الأفراد والسلطات المسؤولة على الفور	72	57.6
تجاهل الامر	53	42.4
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

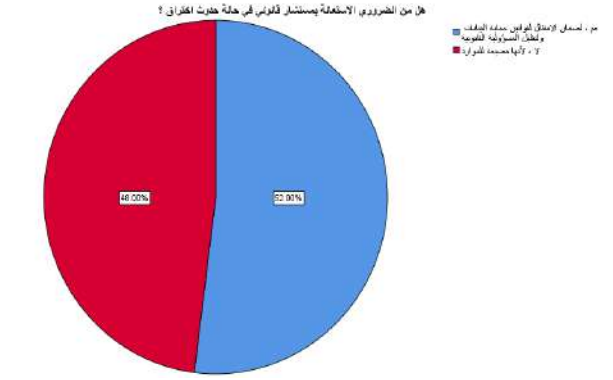
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الخطوة الأولى التي يجب اتخاذها في حالة حدوث اختراق حيث كان فيها "إخطار الأفراد والسلطات المسؤولة على الفور" النسبة الأكبر حيث بلغت هذه النسبة 57.6%بينما قدرت نسبة "تجاهل الامر" 42.4% نستخلص من ذلك ان إخطار الأفراد والسلطات المسؤولة على الفور هوا اول خطوة يتخذها اغلبية المبحثوين و يعود ذلك إلى الإسراع في التحقيقات حيث يتعين على المحققين البدء في التحقيقات بأسرع وقت ممكن لإثبات الجريمة والقبض على الجاني، وهذا يتطلب إخطار السلطات المسؤولة بشكل فوري.

الجدول رقم 30 : ضرورة الاستعانة بمستشار قانوني في حالة حدوث اختراق

الفئات	التكرار	النسبة المئوية
نعم ، لضمان الامتثال لقوانين حماية البيانات ولتقليل المسؤولية القانونية	65	52.0
لا ، لأنها مضيعة للموارد	60	48.0

الشكل رقم 27 : ضرورة الاستعانة بمستشار قانوني في حالة حدوث اختراق

المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب ضرورة الاستعانة بمستشار قانوني في حالة حدوث اختراق حيث كان فيها "نعم ، لضمان الامتثال لقوانين حماية البيانات ولتقليل المسؤولية القانونية" النسبة الأكبر حيث بلغت هذه النسبة 52.0%بينما قدرت نسبة " لا ، لأنها مضيعة للموارد " 48.0%

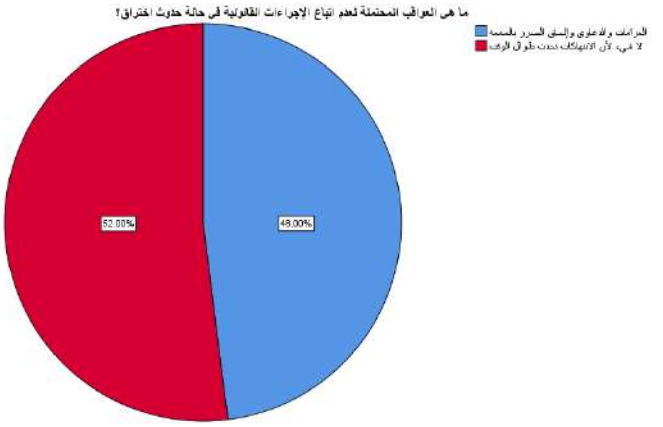
نستخلص من ذلك ان ضرورة الاستعانة بمستشار قانوني في حالة حدوث اختراق هوا امر لازم و يعود ذلك إلى الحصول على المشورة القانونية اللازمة حيث يمكن للمستشار القانوني تزويدك بالمشورة اللازمة حول كيفية التعامل مع الاختراق والتأكد من أنك تتبع الإجراءات القانونية المناسبة.

الجدول رقم 31 : العواقب المحتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق

الفئات	التكرار	النسبة المئوية
الغرامات والدعاوى وإلحاق الضرر بالسمعة	60	48.0

الشكل رقم 28 : العواقب المحتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق

لا شيء لأن الانتهاكات تحدث طوال الوقت	65	52.0
المجموع	**125**	**100.0**



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

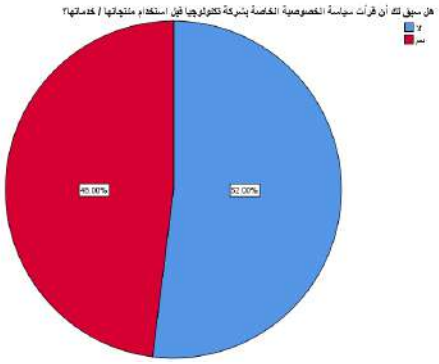
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب هي العواقب المحتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق حيث كانت فيها اجابة "لا شيء لأن الانتهاكات تحدث طوال الوقت" النسبة الأكبر و بلغت هذه النسبة 52.0%بينما قدرت نسبة " الغرامات والدعاوى وإلحاق الضرر بالسمعة" 48.0%

نستخلص من ذلك ان المبحوثين يعتبرون ان لا عواقب محتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق و يعود ذلك إلى غياب الوعي القانوني والتقني بشكل عام

الجدول رقم 32 : قراءة السياسة الخصوصة بشركة تكنولوجيا قبل استخدام خدماتها

الفئات	التكرار	النسبة المئوية
لا	65	52.0
نعم	60	48.0
المجموع	**125**	**100.0**

الشكل رقم 29 : قراءة السياسة الخصوصة بشركة تكنولوجيا قبل استخدام خدماتها



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

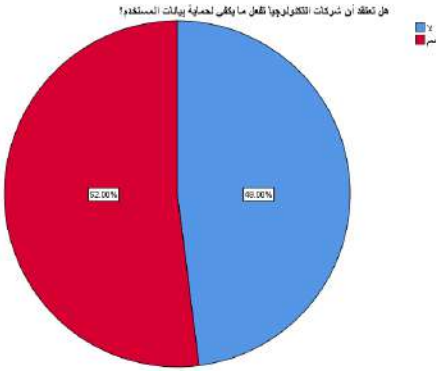
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب قرأة سياسة الخصوصية الخاصة بشركة تكنولوجيا قبل استخدام منتجاتها / خدماتها حيث اغلبية المبحوثين جابوا با لا و بلغت هذه النسبة 52.0%بينما الذين اجابوا با نعم بلغت نسبتهم 48.0

نستخلص من ذلك أن الاغلبية لا يقرؤن سياسة الخصوصية الخاصة بشركة تكنولوجيا قبل استخدام منتجاتها / خدماتها لانهم يعتبرون أن قراءة سياسة الخصوصية مملة وصعبة الفهم، لذلك يميلون إلى تجاهلها

الجدول رقم 33 : شركات التكنولوجيا تفعل ما يكفي لحماية بيانات المستخدم

الفئات	التكرار	النسبة المئوية
لا	60	48.0
نعم	65	52.0
المجموع	**125**	**100.0**

الشكل رقم 30 : شركات التكنولوجيا تفعل ما يكفي لحماية بيانات المستخدم



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الاعتقاد **أن شركات التكنولوجيا تفعل ما يكفي لحماية بيانات المستخدم** حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 52.0%بينما الذين اجابوا با لا بلغت نسبتهم 48.0

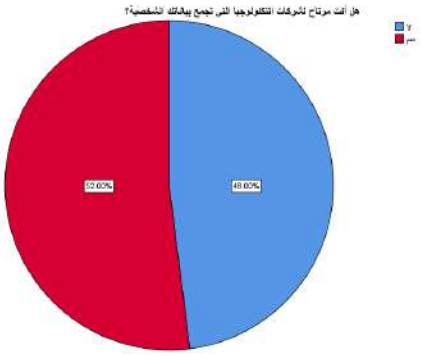
نستخلص من ذلك أن الاغلبية يعتقد ان أن شركات التكنولوجيا تفعل ما يكفي لحماية بيانات المستخدم و يعود ذلك انهم يثقون بالشركات التكنولوجية ويرون أنها تهتم بسمعتها وبالمحافظة على بيانات المستخدمين

الجدول رقم 34 : الارتياح لشركات التكنولوجيا التي تجمع بيانات الشخصية

الفئات	التكرار	النسبة المئوية
لا	60	48.0
نعم	65	52.0
المجموع	125	100.0

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

الشكل رقم 31 : الارتياح لشركات التكنولوجيا التي تجمع بيانات الشخصية



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

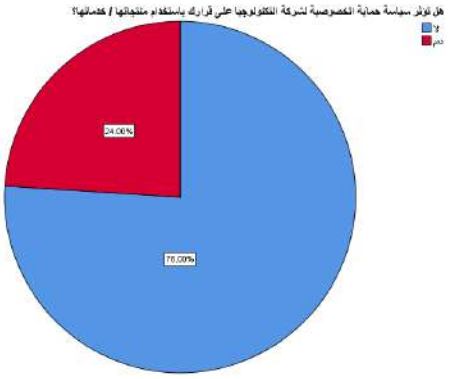
من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب الارتياح لشركات التكنولوجيا التي تجمع بياناتهم الشخصية حيث اغلبية المبحوثين جابوا با نعم و بلغت هذه النسبة 52.0%بينما الذين اجابوا با لا بلغت نسبتهم 48.0

نستخلص من ذلك أن الاغلبية مرتاح لشركات التكنولوجيا التي تجمع بياناتهم الشخصية و يعود ذلك هذه الشركات تقدم خدمات مفيدة ومهمة، والتي يعتبر استخدامها ضروريًا في حياتهم اليومية، ولذلك يرون أن الإفصاح عن بعض المعلومات الشخصية هو سعر بسيط للاستفادة من هذه الخدمات.

الجدول رقم 35 : تأثير سياسة حماية الخصوصية لشركة التكنولوجيا على القرار

الشكل رقم 32 : تأثير سياسة حماية الخصوصية لشركة لشركة التكنولوجيا على القرار

الفئات	التكرار	النسبة المئوية
لا	95	76.0
نعم	30	24.0
المجموع	125	100.0



المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

المصدر: من إعداد الطالبين بالاعتماد على نتائج spss

من خلال قراءتنا للجدول نجد أن توزيع أفراد العينة بحسب تاثير سياسة حماية الخصوصية لشركة التكنولوجيا على قرارهم باستخدام منتجاتها / خدماتها حيث اغلبية المبحوثين جابوا با لا و بلغت هذه النسبة 76.0%بينما الذين اجابوا با نعم بلغت نسبتهم 24.0

نستخلص من ذلك أن الاغلبية لا تؤثر عليه سياسة حماية الخصوصية لشركة التكنولوجيا على قرار باستخدام منتجاتها / خدماتها ذلك لاعتبارهم ان التحكم في البيانات الشخصية معقدًا وغامضًا، مما يجعلهم يفضلون تجاهل سياسة الخصوصية بدلاً من محاولة فهمها

النتائج العامة لدراسة :

تظهر النتائج ان عنصر الاناث هم النسبة الاكبر من طرف الطلبة المبحوثين بالنسبة 69.6% في المقابل نسبة الذكور كانت 30.4%كان سن المبحوثين 21 سنة هم النسبة الاكبر وقد قدرت 28.8% وبعدها نجد 23 سنة بنسبة 22.4% بالمئة

وبعدها سن 20 بنسبة 20% ثم 22 سنة بنسبة 16.8% و اخيرا سن 26 بنسبة 2.4% بالنسبة المستوى الجامعي كانت النسبة النسبة المرتفعة لسنة 3 ليسانس ينسبة 27.2% ثم ثانية ماستر با نسبة 26.4% ثم تليها 2 ليسانس 25.6% و في الاخير سنة اولى ماستر 20.8% بالنسبة لتخصص المبحوثين في قسم الاعلام و الاتصال نجد ان الفئة الاكبر لاتصال الجامهيري 39.2% ثم تليها الاعلام و الاتصال 25.6% و بعدها تخصص الاتصال 24% تليها السمعي البصري بنسبة 8% و في الاخير تخصص الاعلام با نسبة 3.2% نلاحظ ان المبحوثين يستخدمون الفيسبوك بنسبة 49.6% و يرجع ذلك لتنوع المحتوى على هذا الموقع اغلبية المبحوثين يستخدمون مواقع التواصل الاجتماعي يوميا بنسبة 88.8% و هذا بسبب اهتمامهم الكبير بهذا المواقع نلاحظ ان المبحوثين لا يتابعون اي صفحات او مجموعات تتعلق بثقافة المعلومات على مواقع التواصل الاجتماعي بنسبة 84% لانهم يعتبرونها تستخدم للتواصل مع الاصدقاء و العائلة و الاستمتاع بالوقت ان اغلبية المبحوثين لم يتعلموا شيئا جديدا عن ثقافة امن المعلومات من موقع التواصل الاجتماعي بنسبة 80.8% ذلك لعدم اهتمامهم بثقافة امن المعلومات يعتقد افراد العينة ان ان مواقع التواصل الاجتماعي لا تساعد على نشر الوعي بثقافة امن المعلومات بنسبة 81.6% لقصر الرسائل و المنشورات على مواقع التواصل الاجتماعي و هذا غير كافي لتوضيح اهمية ثقافة امن المعلومات اغلب الطلبة المبحوثين تلقوا تعليم رسمي و تدريب على امن المعلومات بنسبة 78.4% و هذا بسبب انه يعتبر احد التحديات الكبيرة التي تواجهها المؤسسات والأفراد في العصر الرقمي الحالي. فمع التطور الكبير لتقنيات الحاسوب وشبكات الإنترنت، أصبح من الضروري حماية المعلومات الحساسة التي يتم تبادلها عبر الإنترنت من الاختراقات والهجمات الإلكتروني نلاحظ ان اغلبية الطلبة المبحوثين لم يتعرضوا لهجوم الكتروني او خرق لبيانات بالنسبة 51.2% لاتباعهم ممرسات الامنية السليمة نرى ان اغلبية الطلبة نادرا ما يقراؤن الاخبار او المقالات المتعلقة بالامن المعلومات بنسبة قدرت 55.2% و \لك لعدم ادراك لاهمية امن المعلومات و خطورة التهديدات التي تواجههم يتضح ان الطلبة المبحوثين حضروا ورشة عمل او ندوة تتعلق بامن المعلومات با نسبة قدرت ب84.4% للحصول على معلومات قيمة عن كيفية حماية بيانتهم يتضح ان اغلب المبحوثين توجهو الى مصادر التجارب الشخصية مع الهجمات الالكترونية او خروقات البيانات للوعي بأمن المعلومات بنسبة 34.4 تعد من اهم المصادر زيادة للوعي في امن المعلومات اغلب الطلاب يعرفون كيف يحمون انفسهم من القرصنة الإلكترونية بنسبة 55.2 بسبب اطلاعهم على اخر تطورات الامنية المبحوثين لم يتخدو اي اجراء امني لي يحمو اجهزتهم بنسبة 68.8 اعتقادا بانهم غير مستهدفين من القرصنة الالكترونية اغلب الطلبة هم على دراية بالتقنيات الشائعة التي يستخدمها المتسللون بنسبة 69.6 ويعود دلك الى انهم لديهم تجارب سابقة مع الاختراق السيبراني وهده التجارب قد تدفعهم الى تعلم كيفية الحماية واتخاد اجراءات الازمة نرى ان اغلبية المبحوثين الطلبة هم على دراية بمفهوم التصيد بنسبة 69.6% لانهم يتلقون حملات توعية تحذرهم من خطر البريد الالكتروني المزيف المبحوثين لم يستخدموا مدير كلمات المرور لتامين كلمات المرور الخاصة بهم بنسبة 57.6% بسبب تفضيلهم كلمات المرور القصيرة و السهلة التذكر نلاحظ ان الطلبة المبحوثين لا يعلمون هجوم رفض خدمة الموزع با نسبة 97.6% و يعود ذلك لقلة الوعي التقني حيث يعود هذا الهجوم الى فهم تقني متطور يتضح ان المبحوثين لا يهتمون بسياسة الخصوصية لتطبيقات بنسبة 76% و يرجع سبب ذلك لغياب الادراك للمخاطر المحتملة و لعدم الاهتمام بسياسات الخصوصية المبحوثين ليسوا على دراية بالمصادقة الثنائية كطبقة امان اظافية بنسبة 51.2% يو يعود سبب ذلك ان لديهم فهم ضعيف للتقنية و الامان الالكتروني مما يجعلهم غير ملمين بأهمية المصادقة الثنائية.

اغلب الطلبة المبحوثين لم يغيرو كلمة المرور بسبب خرق بيانات او حدث امني بنسبة 92.8% بسبب اهمالهم وتأجيله الى وقت اخر يتضح ان اغلبية المبحوثين واثقون في قدراتهم على تحديد و تجنب عمليات التصيد الاحتيالي بنسبة 72.8% بسبب اعتمادهم على برامج مكافحة الفيروسات المبحوثين يستخدمون كلمات المرور قوية بنسبة 67.2 % و يعود سبب ذلك توعية المستخدمين بشكل مستمر من خلال حملات الإعلام والإعلانات والنصائح الأمنية نرى ان المبحوثين لم يبلغو عن رسالة بريد الكتروني مشبوه لقسم تكنولوجيا المعلومات بنسبة52% لعدم ادراكهم لتدابير الامنية التي يجب اتخاذها لحماية انفسهم اغلبية الطلبة المبحوثين عند حدوث اختراق يتخذون اخطار الافراد و السلطات المسؤولة على الفور كخطوة اولى بنسبة 57.6% ذلك لإسراع في اثبات الجريمة و القبض على الجاني يعتبر اغلبية الطلبة ان من الضروري الاستعانة بمستشار قانوني في حالة حدوث اختراق بنسبة 52% لضمان الامتثال لقوانين حماية البيانات و لحصول على المشورة القانونية اللازمة يعتبر اغلبية الطلبة انه لا توجد عواقب المحتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق بنسبة 52% ذلك لغياب الوعي القانوني و التقني بشكل عام نلاحظ ان اغلبية الطلبة المبحوثين لا يقرؤون سياسة الخصوصية الخاصة بشركة تكنولوجيا قبل استخدام منتجاتها / خدماتها بنسبة 52% ذلك لاعتبارهم أن قراءة سياسة الخصوصية مملة وصعبة الفهم يعتقد اغلب المبحوثين ان الشركات التكنولوجية تفعل ما يكفي لحماية بيانات المستخدم بنسبة 52% و يرجع ذلك لثقتهم بهذه الشركات التكنولوجية يتضح ان اغلب الطلبة مرتحاون لشركات التكنولوجيا التي تجمع بياناتهم الشخصية بنسبة 52% بسبب ان الشركات تقدم خدمات مفيدة ومهمة، والتي يعتبر استخدامها ضروريًا في حياتهم اليومية يرى الطلبة المبحوثين سياسة حماية الخصوصية لا تؤثر على قراراتهم بستخدام منتجاتها بنسبة 76% لاعتبارهم ان التحكم في البيانات الشخصية معقدًا وغامضًا

مناقشة نتائج الدراسة :

- ✓ من خلال التساؤل المطروح دور ثقافة أمن المعلومات في الحد من مخاطر الجرائم الإلكترونية، وجدنا أن أغلبية الطلبة المبحوثين لم يتلقو للهجوم الإلكتروني أو إختراق بيانات وذلك بسبب إثباتهم الممارسات الأمنية السليمة.
- ✓ ونلاحظ أيضا أن أغلبية الطلبة هم على ذراية بمفهوم التصيد لأنهم يتلقون حملات توعيهم و تحذرهم من خطر البريد الإلكتروني المزيف.
- ✓ ومن الدوافع أيضا نجد أن هناك دوافع تدفع بعدم الإهتمام بالسياسات الخصوصية، وذلك راجع لسبب غياب الإدراك للمخاطر المحتملة وإعتبار قرائتها صعبة ومملة وصعبة الفهم ولا تؤثر على قراراتهم.
- ✓ ونلاحظ من خلال نتائج على أن أغلب العينة يعتقدون أن الشركات الإلكترونية تفعل مايكفي للحماية البيانات المستخدمة ويرجع ذلك إلى تفهم هذه الشركات التكنولوجية.
- ✓ توعية المستخدمين بشكل مستمر وواضح من خلال إستخدامهم كلمات مرور قوية راجع ذلك للنشر حملات الإعلام والإعلانات والنصائح الأمنية

الخاتمة

خاتمة :

ان الأمن المعلوماتي متعدد الأبعاد والمستويات، حيث يبدأ بتحقيق أمن الدولة ثم المجتمع وأفراده، ويمتد ليشمل كافة الدوائر التي يمكن أن تشكل مصدراً للتهديد. وتزداد أهمية الأمن السيبراني في ظل التطورات الهائلة التي شهدها عالم المعلوماتية، مما جعل المتغيرات الأمنية الإلكترونية حاكمة للعديد من البيانات والقرارات.

فالتهديدات السيبرانية خطراً حاضراً ومستقبلاً الذي أنتجته الحضارة والتقنية والثورة المعلوماتية التكنولوجية، وتؤثر على الدول الضعيفة والمتطورة على حد سواء، وتشكل تهديداً مدمراً لمختلف القطاعات الحيوية والاقتصادية والاجتماعية والسياسية، بما في ذلك الشخصية.

وبناءً على دراستنا، اعتبرنا أنه من المهم توضيح مستوى وعي وإدراك الطلاب لمفهوم الأمن المعلوماتي ومخاطر التهديدات على شبكات التواصل الاجتماعي. ولذلك، قمنا باستخدام مجموعة من الأساليب في دراسة عينتنا التي تتكون من طلاب قسم علوم الإعلام والاتصال بجامعة قاصدي مرباح ورقلة. باعتبار ان الأمن المعلوماتي مفهوماً أساسياً في ظل التطور الهائل في مجال التكنولوجيا والاتصالات، ويجب على الناس معرفة القوانين والنظم والطرق والأساليب لمواجهة الجرائم الإلكترونية.

علماً بأن نتائج دراستنا تخص فقط طلاب علوم الإعلام والاتصال بجامعة قاصدي مرباح ورقلة، ولا يمكن تعميمها على جميع طلاب الجامعات الجزائرية.

قائمة المراجع

قائمة المراجع :

اولا :الكتب :

1. ابراهيم ابرش. المنهج العلمي و تطبيقاته في العلوم الاجتماعية. دار الشروق لنشر و التوزيع. عمان.
2. بلقاسم سلطانية ,حسان الجيلاني , المناهج الأساسية في البحوث الاجتماعية ,ط1,دار الفجر القاهرة ,2012
3. جابو ربي مصطفى، المعج الوسيط، المكتبة الاسلامية للطباعة والنشر، القاهرة، 1972
4. خالد ممدوح . امن الجريمة الالكترونية. الدار الجامعية. الالكترونية. الاسكندرية .2008.
5. رشد زواتي . منهجية البحث العلمي في غلوم العلوم الاجتماعية \ اسس علمية و تدريبات \ . دار الكتاب الحديث . القاهرة. 2004.
6. ضياء مصطفى عثمان. السرقة الالكترونية. دار النفائس. عمان. الطبعة الاولى. 2011.
7. عبد الرحمن بن زيد الزنيدي، المثقف العربي بين العصرانية والإسلامية، ط1، دار كنوز اشبيليا للنشر، الرياض، السعودية، 2009
8. عبد الرزاق الدليمي: ‘‘نظريات الاتصال في القرن الحادي والعشرين "، دار اليازوري العلمية، ط1، عمان، الأردن، 2016
9. محمد الصاوى محمد مبارك ,البحث العلمي أسسه وطريقة كتابته ,ط1 المكتبة الأكاديمية ,القاهرة ,1992
10. محمد سرحان علي المحمودي, مناهج البحث العلمي ,دار الكتب , صنعاء, اليمن, ط3, 2015
11. المنجد في اللغة و الأعلام ،ط43، دار المشرق ،لبنان،2008
12. مورس انجرس، منهجية البحث العلمي في العلوم الانسانية، ترجمة صحراوي بوزيد، ط 2، دار القصبة لنشر. الجزائر . 2004.
13. موريس أنجرس، منهجية البحث العلمي في العلوم الإنسانية تدريبات علمية، ط2، تر: بوزيد صحراوي وآخرون، دار القصبة للنشر، الجزائر، 2006
14. نادية سعيد عيشور، منهجية البحث العلمي في العلوم الاجتماعية، مؤسسة حسين رأس الجبل للنشر، الجزائر، 2017
15. نادية عيشور وآخرون ،منهجية البحث العلمي في العلوم الاجتماعية ، مؤسسة حسين راس الجبل للنشر و التوزيع ،الجزائر،2017.

ثانيا: المقالات و المجلات

16. إبن المنظور ،لسان العرب ،جزء 16، وزارة الشؤون الإسلامية والأوقاف و الدعوة و الإرشاد، السعودية
17. احمد بن مرسلي .. مناهج البحث العلمي في الاعلام و الاتصال. ديوان المطبوعات الجامعية . بن عكنون. الجزائر.2003.
18. بخي فاطمة الزهراء . اجراءات التحقيق في الجريمة الالكترونية . 2014.
19. بوسعيد رندا: ‘‘التغير الاجتماعي والحتمية التكنولوجية لوسائل الإعلام، قراءة في نظرية مارشال ماكلوهان، العدد 1، 2011، جامعة الجلفة، الجزائر.
20. تواتي نور الدين: "مجلة العلوم الإنسانية والاجتماعية، ماكلوهان مارشال قراءة في نظريته بين الأمس واليوم"، العدد العاشر، مارس 2013، جامعة الجزائر 3 الجزائر.
21. محمود حسن الصاحب،سياسة أمن المعلومات في الجامعات حالة درسة،cybrarians journal ،ع33،القاهرة ،2013

ثالثا : المذكرات و الرسائل الجامعية :

22. أحمد مرسلي، منهج البحث العلمي في علوم الاعلام والاتصال، ديوان المطبوعات الجامعية،الجزائر

23. زهرة بزاوية ،مجتمع المعلومات والكفاءات الجديدة لدى أخصائي المعلومات،"دراسة ميدانية بالمؤسسات الوثائيقية لولاية وهران" مذكرة لينيل شهادة الماجستير في علم المكتبات والعلوم الوثائقية،جامعة وهران،2014-2015 ،ص15،نقلا عن عمر أحمد همشري ،المكتبة ومهارات استخدامها،دار صفاء ، الاردن

قائمة الملاحق

جامعة قاصدي مرباح–ورقلة–
كلية العلوم الإنسانية والاجتماعية
قسم علوم الإعلام والاتصال
تخصص اتصال جماهيري والوسائط الجديدة

استمارة استبيان

دور ثقافة الأمن المعلوماتي في الحد من مخاطر الجرائم الالكترونية
دراسة على عينة من قسم علوم الإعلام والاتصال

بعد التحية والتقدير

نضع بين أيدي المبحوثين المحترمين استمارة خاصة ببحث علمي ميداني، لتحضير شهادة ماستر حول الموضوع المذكور أعلا، كما نحيطكم علما أن هذه الاستمارة تحتوي على مجموعة أسئلة فالرجاء منكم القراءة المتأنية للأسئلة والإجابة عليها حسب ما هو موجود من معلومات مقدمة في محاور الدراسة، كما أنها تستعمل لأغراض علمية بحتة.

إعداد الطلبة:
بوعبون رضوان
جزار حمزة حسام الدين

تحت إشراف:
د.بودربالة عبد القادر

البيانات الشخصية :
الجنس:
ذكر ☐ أنثى ☐
السن:
.....

المستوى الجامعي :
سنة ثانية ليسانس ☐
سنة ثالثة ليسانس ☐
سنة اولى ماستر ☐
سنة ثانية ماستر ☐

التخصص:
الاتصال ☐ إعلام ☐ إعلام و اتصال ☐
اتصال جماهيري ☐ السمعي البصري ☐

المحور الاول : المصادر المسؤولة عن تشكيل ثقافة أمن المعلوماتي لدى الطلبة الجامعيين

1- ما هي مواقع التواصل الاجتماعي التي تستخدمها؟
- فيسبوك ☐
- إنستغرام ☐
- تيك توك ☐
- سناب شات ☐

2- كم مرة تستخدم مواقع التواصل الاجتماعي؟
- يوميًا ☐
- أسبوعيًا ☐
- شهريًا ☐

3- هل تتابع أي صفحات أو مجموعات تتعلق بثقافة المعلومات على مواقع التواصل الاجتماعي؟
- نعم ☐
- لا ☐

4- هل تعلمت شيئًا جديدًا عن ثقافة المعلومات من مواقع التواصل الاجتماعي؟

نعم ☐

لا ☐

5- هل تعتقد أن مواقع التواصل الاجتماعي يمكن أن تساعد في نشر الوعي بأهمية ثقافة المعلومات؟

نعم ☐

لا ☐

6- هل تلقيت أي تعليم رسمي أو تدريب على أمن المعلومات؟

نعم ☐ لا ☐

7 هل سبق لك أن تعرضت لهجوم إلكتروني أو خرق للبيانات؟

نعم ☐ لا ☐

8 كم مرة تقرأ الأخبار أو المقالات المتعلقة بأمن المعلومات؟

يوميًا ☐

أسبوعي ☐

شهريا ☐

نادرًا ☐

أبداً ☐

9 هل سبق لك أن حضرت ورشة عمل أو ندوة تتعلق بأمن المعلومات؟

نعم ☐ لا ☐

10أي من المصادر التالية ساعدك في أن تصبح أكثر وعياً بأمن المعلومات ؟

التعليم / التدريب الرسمي ☐

التغطية الاخبارية والاعلامية ☐

التجارب الشخصية مع الهجمات الإلكترونية أو خروقات البيانات ☐

المنتديات والمناقشات عبر الإنترنت ☐

الأصدقاء والعائلة ☐

المحور الثاني : مدى إطلاع الطالب على أساليب وطرق الاختراق الالكتروني

11- هل تعرف كيف تحمي نفسك من القرصنة الإلكترونية؟

نعم ☐

لا ☐

12- هل سبق لك أن اتخذت أي إجراءات لتأمين جهازك (أجهزتك) ضد القرصنة الإلكترونية؟

نعم ☐

لا ☐

13- هل أنت على دراية بالتقنيات الشائعة التي يستخدمها المتسللون للوصول غير المصرح به إلى الأجهزة الإلكترونية؟

نعم ☐

لا ☐

14- هل يمكنك تحديد ما هو المقصود بـ "التصيد"؟

نعم ☐

لا ☐

لست متأكد ☐

15- هل سبق لك استخدام مدير كلمات المرور لتأمين كلمات المرور الخاصة بك؟

نعم ☐

لا ☐

16- هل تعرف ما هو هجوم رفض خدمة الموزع (DDoS)؟

نعم ☐

لا ☐

المحور الثالث : معرفة الطالب بكيفية حماية بياناته على مواقع الويب المختلفة

17- هل تهتم بسياسات الخصوصية للتطبيقات أو مواقع الويب التي تستخدمها؟

نعم ☐

لا ☐

18- هل أنت على دراية بالمصادقة الثنائية كطبقة أمان إضافية؟

نعم ☐

لا ☐

19- هل سبق لك أن غيرت كلمة مرورك بسبب خرق بيانات أو حادث أمني؟

نعم ☐

لا ☐

20- هل انت واثق في في قدرتك على تحديد وتجنب عمليات التصيد الاحتيالي وغيرها من الأنشطة الاحتيالية عبر الإنترنت؟

نعم ☐

لا ☐

21- ما هي الإجراءات التي تتخذها لحماية معلوماتك الشخصية على الإنترنت؟

استخدم كلمات مرور قوية ☐

تجنب استخدام شبكات Wi-Fi العامة ☐

استخدم برنامج مكافحة فيروسات ☐

اقوم بتحديث البرامج والتطبيقات بانتظام ☐

تحقق من إعدادات الخصوصية على منصات التواصل الاجتماعي ☐

22- هل أبلغت يومًا عن رسالة بريد إلكتروني أو موقع ويب مشبوه لقسم تكنولوجيا المعلومات أو فريق الأمان؟

نعم ☐

لا ☐

23- ما هي الخطوة الأولى التي يجب اتخاذها في حالة حدوث اختراق؟

إخطار الأفراد والسلطات المسؤولة على الفور ☐

تجاهل الامر ☐

24- هل من الضروري الاستعانة بمستشار قانوني في حالة حدوث اختراق ؟

☐

نعم ، لضمان الامتثال لقوانين حماية البيانات ولتقليل المسؤولية القانونية

لا ، لأنها مضيعة للموارد ☐

25- ما هي العواقب المحتملة لعدم اتباع الإجراءات القانونية في حالة حدوث اختراق؟

الغرامات والدعاوى وإلحاق الضرر بالسمعة ☐

لأن الانتهاكات تحدث طوال الوقت ☐

26- هل سبق لك أن قرأت سياسة الخصوصية الخاصة بشركة تكنولوجيا قبل استخدام منتجاتها / خدماتها؟

نعم ☐

لا ☐

27- هل تعتقد أن شركات التكنولوجيا تفعل ما يكفي لحماية بيانات المستخدم؟

نعم ☐

لا ☐

28- هل أنت مرتاح لشركات التكنولوجيا التي تجمع بياناتك الشخصية؟

نعم ☐

لا ☐

29- هل تؤثر سياسة حماية الخصوصية لشركة التكنولوجيا على قرارك باستخدام منتجاتها / خدماتها؟

نعم ☐

لا ☐