وزارة التعليم العالي والبحث العلمي

جامعة يحيى فارس بالمدية

كلية العلوم الإنسانية والاجتماعية

عنوان:

الوعي الأمني وعلاقته بالجريمة المعلوماتية في المجتمع الجزائري

دراسة في جامعة يحيى فارس بالمدية

مذكرة ضمن متطلبات نيل شهادة الماستر في علم اجتماع

تخصص: جريمة وانحراف

من إعداد:

- لطفي بن علي

تحت اشراف الدكتور:

أ.د محمد بناولة

السنة الجامعية: 2024/2023

شكر وعرفـــــــان

قال الله تعالى:

(فَاذْكُرُونِي أَذْكُرْكُمْ وَاشْكُرُوا لِي وَلَا تَكْفُرُونِ)

فالحمد الله الذي وفقنا لإتمام هذا العمل

وعملا بقول رسول الله صلى الله عليه وسلم

{من لم يشكر الناس لم يشكر الله}

الحمد الله الذي بنعمته تتم الصالحات، والشكر له أولا وقبل كل شيء أن أمدنا بالعون والصبر لإتمام

هذا العمل.

نتقدم بجزيل الشكر والتقدير إلى الأستاذ المشرف **د. محمد بناولة**

الذي لم يبخل علينا بتوجيهاته ونصائحه القيمة.

شكرنا موصول لكل من أساتذتي الأفاضل، أساتذة كلية العلوم الإنسانية والاجتماعية، كل باسمه ومقامه.



إهـــداء

أهدي عملي هذا الى

إلـــــــــى

كل عائلتـــــي، وزملائـــــي والأصدقـــاء وكل من كان لهم الأثر في

الكثير من العقبـات والصعـــــاب.

إلـــى جميـع اساتذتـــي الكـــرام

لطفي

فهرس المحتويات:

شكر وعرفـــــان 2

إهـــــداء 3

فهرس المحتويات:..... 3

قائمة الجداول: 8

مقدمة .....أ

الفصل الأول: الإطار المنهجي للدراسة 1

تمهيد: 1

1. الإشكالية:..... 1

2. الفرضيات: 2

3. أهداف الدراسة: 3

4. أهمية الموضوع: 3

5. أسباب اختيار الموضوع:..... 4

6. تحديد المفاهيم: 4

7. الدراسات السابقة: 7

8. المقاربة النظرية: 8

خلاصة الفصل: 10

الفصل الثاني : الجريمة المعلوماتية..... 12

تمهيد: 12

المبحث الأول: مفهوم الجريمة المعلوماتية 13

المطلب الأول: تعريفها 13

أولا: التعريف الفقهي 13

ثانيا: تعريف القانوني 14

المطلب الثاني: تاريخها.....14

المبحث الثاني: الجريمة المعلوماتية ومظاهرها..... 16

المطلب الأول : أسباب الجريمة المعلوماتية 16

المطلب الثاني: مظاهر الجريمة المعلوماتية 18

المبحث الثالث: أثار الجريمة المعلوماتية 19

المطلب الأول: أثرها على الفرد.....19

المطلب الثاني: أثرها على المجتمع.....21

خلاصة الفصل: 23

الفصل الثالث: الوعي الأمني..... 25

تمهيد: 25

المبحث الأول: الوعي الأمني وأهميته 26

المطلب الأول: مفهوم الوعي الأمني.....26

أ _ الوعي الأمني باعتباره إدراك للمبادئ والقواعد الأمنية: 26

ب-الوعي الأمني باعتباره حالة وجدانية:.....28
المطلب الثاني: أهمية الوعي الأمني 28
1-أهمية الوعي الأمني للفرد: 29
2- أهمية الوعي الأمني للمجتمع:.....30
3-أهمية الوعي الأمني على المستوى الدولي: 30
المبحث الثاني: مؤسسات التنشئة الاجتماعية والوعي الأمني..... 31
المطلب الأول: مؤسسات التنشئة الاجتماعية والوعي الأمني 31
تعريف التنشئة الاجتماعية:.....31
المطلب الثاني: اختلال التنشئة والوعي الأمني.....35
المبحث الثالث: الوعي الأمني ومكافحة الجريمة المعلوماتية..... 37
المطلب الأول: تأثير الوعي الأمني على تقليل الجريمة المعلوماتية 37
المطلب الثاني: مكافحة الجريمة المعلوماتية في التشريع الجزائري 38
أولا: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحتها. 39
ثانيا: الحماية في قانون العقوبات.....39
ثالثا: الحماية في القوانين الخاصة.....40
خلاصة الفصل: 42
الفصل الرابع: الإجراءات المنهجية للدراسة..... 44
الخاتمة العامة.....113
التوصيات 113

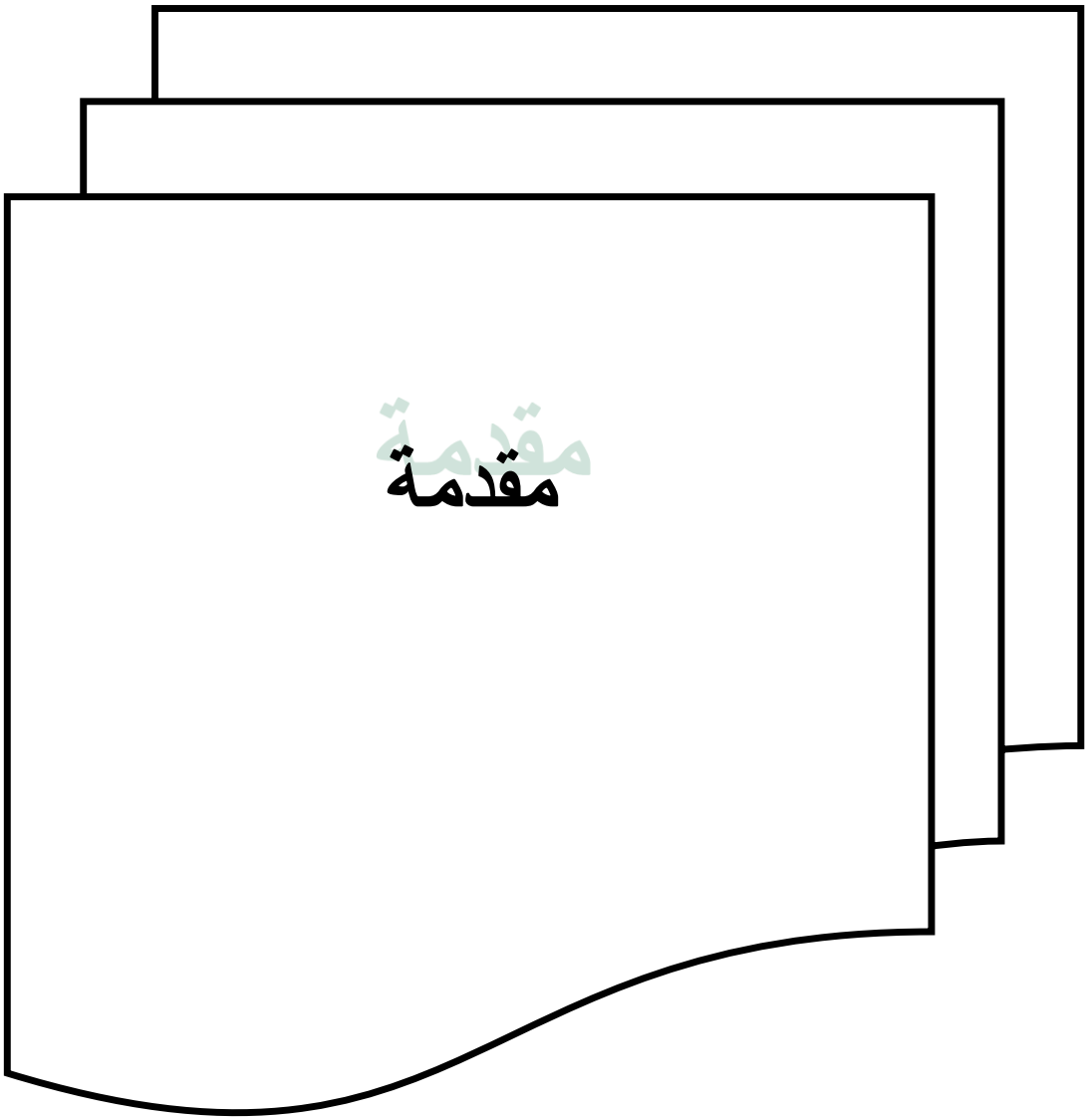
النتائج والاستنتاجات ..... Erreur ! Signet non défini.

قائمة المراجع: 116

قائمة الجداول:

1.جدول رقم (01) يبين توزيع أفراد العينة حسب الفئة العمرية: 45
2.جدول رقم 02 يبين توزيع أفراد العينة حسب الجنس 49
3.جدول رقم 03 يبين توزيع أفراد العينة حسب المستوى الجامعي 52
4.جدول رقم 04 يبين توزيع أفراد العينة حسب البيئة الجغرافية 56
5.جدول رقم 05 يبين العلاقة بين الجنس والتعرض للاختراق الالكتروني 60
6.جدول رقم 06 بين العلاقة بين إتقان استعمال الوسائط التكنولوجية والتعرض للاختراق الالكتروني 64
7.جدول رقم 07 يبين العلاقة بين التصريح بالهوية الكترونيا والتعرض للاختراق الالكتروني 68
8.جدول رقم 08 يبين العلاقة بين التعرض للاختراق الالكتروني ومدى خوف المبحوثين للاختراق 73
9.جدول رقم 09 يبين العلاقة بين التعرض للاختراق الالكتروني وسبب الاختراق من منظور المبحوثين 77
10.جدول رقم (10) يبين العلاقة بين الفئة العمرية للمبحوثين التعرض للاختراق الإلكتروني 80
11.جدول رقم (11) يبين العلاقة بين المستوى الجامعي للمبحوثين التعرض للاختراق الإلكتروني 84
12.جدول رقم (12) يبين العلاقة بين المستوى الجامعي للمبحوثين والمداومة على التجوال في الحقل المعلوماتي 87

13.جدول رقم (13) يبين العلاقة بين الفئة العمرية للمبحوثين والمداومة على التجوال في الحقل المعلوماتي 91
14.جدول رقم (14) يبين العلاقة بين الفئة العمرية للمبحوثين والتصريح بالهدية إلكترونيا 94
15.جدول رقم (15) يبين رأي المبحوثين في الغاية من الاختراق: 97
16.جدول رقم (16) يبين رأي المبحوثين من المتسبب في الاختراق:..... 101
17.جدول رقم (17) يبين رأي المبحوثين في الغاية من الحسابات الوهمية: 104
18.جدول رقم (18) يبين العلاقة بين إتقان استعمال الوسائط التكنولوجية الرأي في قلة وعي مستعملي الوسائط في المجتمع الجزائري 108



مقدمة

مقدمة

في العصر الرقمي الذي نعيشه اليوم، أضحى العالم أشبه بقرية صغيرة مترابطة عبر شبكة الانترنت والتكنولوجيا الرقمية، أصبح الاعتماد على التكنولوجيا جزءا لا يتجزأ من حياتنا اليومية، سواء في العمل أو التعليم أو حتى في الترفيه والتواصل الاجتماعي. ومع هذا الاعتماد المتزايد، ظهرت مخاطر جديدة تتعلق بأمن المعلومات، وأبرزها الجرائم المعلوماتية التي تتنوع بين سرقة الهوية، الاحتيال المالي، الهجمات الالكترونية والبرمجيات الخبيثة.

الوعي الأمني يعد خط الدفاع الأول والأهم ضد هذه الجرائم، فهو يشمل معرفة الأفراد بالمخاطر الأمنية المحتملة، والإجراءات الوقائية التي يجب اتخاذها لحماية أنفسهم ومعلوماتهم الشخصية في الجزائر، كما هو الحال في العديد من الدول يشهد استخدام التكنولوجيا انتشارا سريعا مما يجعل الوعي الأمني قضية حيوية لحماية المجتمع من تهديدات الجرائم المعلوماتية.

على الرغم من الجهود المبذولة لتعزيز الوعي الأمني في الجزائر، لازال هناك فجوات كبيرة تؤدي إلى تعرض الأفراد والمؤسسات لمخاطر أمنية كبيرة، نقص التوعية والتدريب الكافي وضعف السياسات الأمنية، وتدني مستوى الوعي بين المستخدمين، كلها عوامل تسهم في زيادة معدلات الجرائم المعلوماتية

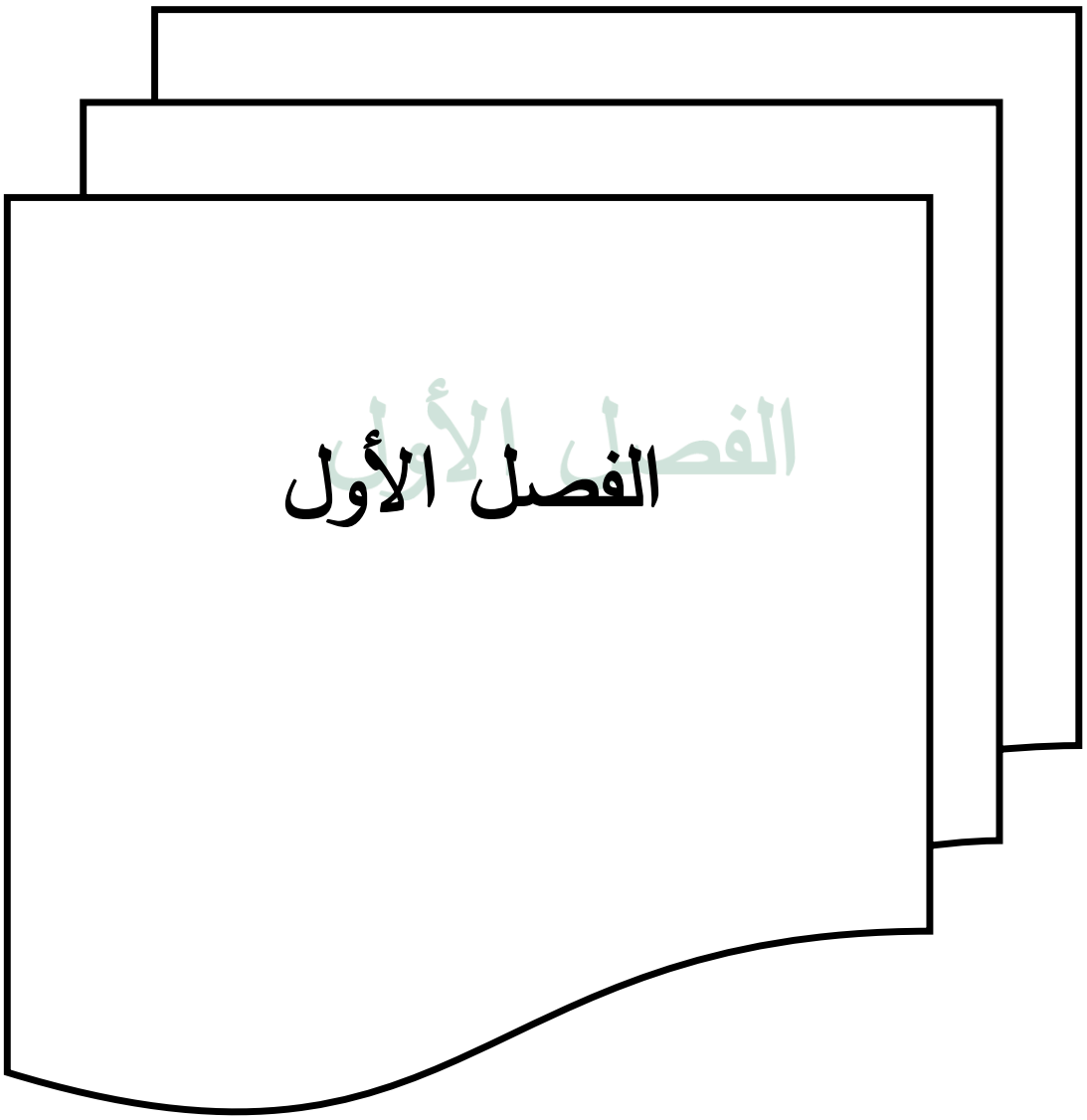
ومن هنا وبناءا على ما سبق ذكره فقد تم تقسيم هذا العمل إلى أربعة فصول:

الفصل الأول: الإطار المنهجي للدراسة وتم فيه التعريف بموضوع الدراسة من حيث تحديد الإشكالية وفرضياتها، كما بين الأسباب، الأهمية والأهداف التي من خلالها تم اختيار هذه الدراسة وتحديد أهم مفاهيمها ومصطلحاتها.

الفصل الثاني: تناول هذا الفصل كل الجوانب المتعلقة بالجريمة المعلوماتية من مفهوم وتاريخها والأسباب ومظاهر الجريمة المعلوماتية وأيضا آثارها والمتمثلة في الآثار على الفرد والمجتمع.

الفصل الثالث: تناولنا في هذا الفصل مفهوم، أهمية الوعي الأمني ومؤسسات التنشئة الاجتماعية واختلالها بالوعي الأمني كما تطرقنا أيضا إلى الوعي الأمني ومكافحته للجريمة المعلوماتية من خلال تأثيره ومن خلال المشرع الجزائري.

الفصل الرابع: الاتجاه التطبيقي لهذه الدراسة، الإحصائيات والنتائج التي تم التوصل إليها من خلال هذه الدراسة.


الفصل الأول

الفصل الأول: الإطار المنهجي للدراسة

تمهيد:

نخصص هذا الفصل بتقديم موضوع الدراسة، ومن خلاله نحاول إعطاء نظرة واضحة حول ما نريد دراسته وتحديد الموضوع تحديدا دقيقا وهذا لتتكين المستطلعين على هذه الدراسة من فهم ما يريد الباحث أن يدرسه بالضبط، والمعلومات الواردة فيه ويعتبر هذا الفصل مهما جدا بالنسبة للبحث ككل باعتباره حجر الأساس الذي سيبنى عليه الباحث أفكاره طوال البحث، وقد تم صياغة إشكالية الدراسة وتساؤلاتها التي من خلالها سيتم الإجابة عنها مؤقتا من خلال الفرضيات، مع تحديد أسباب اختيار الموضوع الوعي الأمني وعلاقته بالجريمة المعلوماتية في المجتمع الجزائري مع إبراز الأهمية والأهداف والمفاهيم المعتمدة في هذا البحث.

1. الإشكالية:

ساهم التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي والزيادة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة من أشخاص طبيعية أو هيئات أو أشخاص معنوية.

في الضوء التوسع في استخدام وسائل التقنية الحديثة ووسائل التواصل الاجتماعي انتشرت عادة استخدام غير اللائق لمختلف تلك الوسائل، وظهرت معها الجرائم المعلوماتية التي فرضت نفسها على المستويين الوطني والعالمي.

كل ذلك أسهم في ظهور فئة جديدة من الإجرام مرتبطة بالتكنولوجيا ومنها جرائم معلوماتية ونظرا لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة الأمر الذي أدى إلى انعكاسها على مضمون الأنظمة والقوانين حيث ثقفت المؤسسات المواطنين من طرق الوعي الأمني حول السياسات والإجراءات المؤسسية ليمكنهم من اكتشاف التهديدات الأمنية التي تواجههم.

الوعي الأمني يلعب دورا كبيرا وحاسما في الحد من الجريمة المعلوماتية حيث يساعد على توعية الأفراد بالمخاطر المحتملة وكيفية حماية أنفسهم ومع ذلك تظل الجريمة المعلوماتية تحديا مستمرا نظرا للتطور التكنولوجي المستمر والتكتيكات المتطورة للمجرمين الإلكترونيين.

وبناء عليه كانت الحاجة ملحة لوضع هذا الموضوع موضوع الدراسة والتحليل.

التساؤلات:

السؤال الرئيسي:

_ كيف يؤثر مستوى الوعي الأمني في المجتمع الجزائري على انتشار الجريمة المعلوماتية؟

الأسئلة الفرعية:

1. ماهو مستوى الوعي الأمني لدى مختلف فئات المجتمع الجزائري؟
2. ماهي أنواع الجرائم المعلوماتية الأكثر شيوعا في الجزائر؟

2. الفرضيات:

أ- الفرضية الرئيسية:

يؤدي انخفاض مستوى الوعي الأمني في المجتمع الجزائري إلى زيادة انتشار الجريمة المعلوماتية حيث يكون الأفراد الأقل وعيا بالأمن الرقمي أكثر عرضة للجرائم بالمقابل يمكن لمستوى الوعي الأمني مرتفع أن يساهم في تقليل معدلات الجريمة المعلوماتية من خلال تعزيز الممارسات الأمنية.

ب- الفرضيات الفرعية:

1 مستوى الوعي الأمني يختلف بشكل كبير بين الفئات العمرية والتعليمية والاجتماعية في المجتمع الجزائري.

2 الاحتيال الالكتروني وسرقة الهوية والابتزاز الالكتروني هي الأكثر شيوعا في الجزائر.

3. أهداف الدراسة:

_معرفة الأثر الذي تتركه الجرائم المعلوماتية على المجتمع.

_ توعية المجتمع من خطورة هذه الجريمة والنتائج التي تقع من وراء حدوثها.

_إيجاد حلول للحد من خطورة هذه الظاهرة.

_فهم كيفية تأثير هذه الجرائم على المجتمع والفرد

_معرفة دور الوعي الأمني وكيفية مساهمته في الحد من انتشار الجريمة.

4. أهمية الموضوع:

_ أهمية دراستنا هي:

_تعالج ظاهرة خطيرة وهي ظاهرة الجرائم المعلوماتية التي تهدد المجتمع وتعرض حياة أفراده للخطر.

_التعرف على أهم العوامل التي تؤدي إلى الجرائم المعلوماتية وكيفية الحد منها عن طريق الوعي الأمني.

_تحديد أنواع الجرائم المعلوماتية وأيها أكثر انتشارا.

5. أسباب اختيار الموضوع:

_ التفشي والانتشار الكبير للجرائم المعلوماتية في الآونة الأخيرة في العالم عامة والمجتمع الجزائري خاصة.

_تردد الآراء حول أسباب الجرائم المعلوماتية.

_ الميل الشخصي إلى المواضيع المتعلقة بالجريمة.

_الرغبة في فهم الأسباب التي تقع وراء هذه الجرائم.

_ الحاجة إلى تحذير وتوعية المجتمع عامة بمخاطر هذه الجرائم وكيفية تجنبهم للوقوع كضحايا لها.

_الرغبة في الإسهام في تطوير المجتمع

6. تحديد المفاهيم:

تعبر المفاهيم العلمية ضرورية منطقية في أي بحث أن دراسة فهي مفاتيح أساسية كل دراسة.

و سوف نتطرق إلى هذه المفاهيم قبل الدخول في صلب الموضوع وتحديد تعاريف مثل (الوعي، الأمن، الوعي الأمني، الجريمة، الجريمة المعلوماتية)

وفي الفصول نقدم تعاريف مفصلة لهم.

1. الوعي:

أ تعريف اللغوي:

وعى، الوعي، حفظ القلب الشيء أو الحديث يعيه وعيا وأوعاه، حفظه وفهمه، وقبله، فهو واع، فلان أوعى من فلان، أي أحفظ وأفهم.

ب التعريف الاصطلاحي:

الوعي هو إتجاه عقلي انعكاسي يمكن للفرد من الوعي بذاته وبالبيئة المحيطة به بدرجات متفاوتة من الوضوح أو التعقيد، يتضمن وعي الفرد لوظائفه العقلية والجسمية ووعيه بالأشياء والعالم الخارجي.[1]

2. الأمن:

أ- التعريف اللغوي:

الأمن مضاده الخوف والفزع، فهو يعني الطمأنينة والاطمئنان إلى عدم توقع المكروه، وربط الإسلام الأمن بالإيمان ولذلك دعا الله عز وجل عباده إلى الأيمان به ليتحقق لهم الأمن والأمان.[2]

ب- التعريف الاصطلاحي:

يعرف بأنه حالة أو شعور بالطمأنينة والاستقرار والحرية من الخوف والتهديدات، سواء كانت هذه التهديدات ذات طبيعة داخلية أو خارجية، مادية أو معنوية.

يشمل الأمن الحفاظ على سلامة الأفراد والمجتمع من المخاطر التي يمكن أن تهدد حياتهم أو ممتلكاتهم أو قيمهم، يمكن أن يكون الأمن على مستوى الأفراد (الأمن الشخصي) أو على مستوى الدول (الأمن القومي)، ويتحقق من خلال سياسات وإجراءات وقوانين تهدف إلى حماية الحقوق الأساسية وتوفير البيئة الملائمة للنمو والازدهار.[3]

3. الوعي الأمني:

---

[1] فاروق مداس ، قاموس مصطلحات علم الاجتماع ، الجزائر ، دار مدني للطباعة والنشر، 2003 ، ص296

[2] محمد عمارة، مقومات الأمن الاجتماعي في الإسلام،القاهرة،مصر، مكتبة الإمام البخاري، الطبعة الأولى ،2009 ، ص 90

[3] جامعة محمد خيضر .2013 ، ص 10 أمينة دير ،أثر التهديدات البيئة على واقع الأمن الإنساني في إفريقيا دراسة حالة،

يرى بعض الباحثين أن الوعي الأمني يتحقق بإدراك الفرد للمبادئ والأحكام الأمنية وما يترتب عليها من ممارسة للقواعد الأمنية، ويرى آخرين أن الوعي الأمني يتعلق بالجانب الوجداني لدى الفرد والمتمثل في الشعور بالخطر والرغبة في الشعور بالأمان، ويقصد به إحدى العمليات الذهنية التي تعطي الإنسان القدرة على التبصر بالمعلومات الأمنية ومعرفة نتائج ما يقدم عليه من أفعال إرادية، والبحث المستمر حول ما لا يعرفه من هذه النتائج حتى يصل إلى تحديدها.[1]

4. الجريمة:

الجريمة هي سلوك انحرافي وجنوح طارئ لارتكاب عمل ممنوع ارتكابه

التعريف اللغوي للجريمة:

فمن الناحية اللغوية أخذت كلمة جريمة من المجرم: التعدي والجرم هو الذنب، والجمع إجرام وجروم، وهو الجريمة، ويقال جلرم فلان أذنب وأخطأ فهو مجرم وجريم.[2]

التعريف الاصطلاحي للجريمة:

هي عدوان شخص على أخر في عرضه أو ماله أو متاعه أو شخصه، إنها بهذا المعنى تعتبر ظاهرة اجتماعية لا يخلو منها مجتمع، فحيث توجد حياة اجتماعية توجد جريمة.[3]

5. الجريمة المعلوماتية:

[1] العمري ،عبد الله بن محمد ، دور الثقافة الأمنية في الوقاية من الفكر المتطرف في المجتمع السعودي، الرياض 2014 ،ص 37

[2] }امعة نايف العربية للعلوم الأمنية ، السعودية، 2011، ص 28 أسماء بنت عبد الله بن عبد المحسن التويجري، الخصائص الاجتماعية والاقتصادية للعائدات للجريمة،

[3] ، مجلة الآداب ، الجامعة المستنصرية ، ص 391 يحي خير الله عودة، البيئة والسلوك الإجرامي(دراسة نظرية في الإنثروبولوجيا الجنائية

وصفت الجريمة المعلوماتية بأنها جريمة تقاوم التعريف، نتيجة اختلاف التعريفات وتفاوتها حيث تعددت الآراء والأفكار بشأن المفهوم، فهناك من اعتمد في تعريفه على الجانب الفني وهناك من اعتمد على الجانب القانوني وهناك من اعتمد على معايير أخرى مختلفة ومن بين هذه المحاولات التعريف الصادر عم منظمة التعاون الاقتصادي للتنمية OCDE حيث عرفت الجريمة المعلوماتية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال والمعنوية، يكون ناتجا يطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.

و صفوة القول فإن مفهوم الجريمة المعلوماتية يكتنفه العديد من الصعوبات كونه يستخدم لوصف طائفغة واسعة من الأفعال الإجرامية.[1]

7. الدراسات السابقة:

الدراسة الأولى:

_ رسالة ماجستير " الإطار القانوني لمكافحة الجريمة المعلوماتية في التشريع الجزائري" جامعة باتنة، كلية الحقوق والعلوم السياسية، عبد اللطيف معتوق سنة 2011 / 2013

الدراسة الثانية:

_ دراسة بعنوان: قياس مستوى الوعي الأمني السيبراني للجرائم الإلكترونية في المملكة العربية السعودية 2021.

أهم نتائجها: أن 32.5% من عينة الدراسة ليس لديهم أي فكرة عن هجمات التصيد الاحتيالي.

الدراسة الثالثة:

[1] مصر ،2005، ص 96 أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي

_ دراسة المطوع 2020 بعنوان: مستوى الوعي لدى طلبة كلية التربية بجامعة شقراء بنظام مكافحة الجرائم المعلوماتية والتدابير التربوية لزيادته.

وسعت الدراسة إلى معرفة مستوى الوعي الأمني بنظام مكافحة الجرائم المعلوماتية عند طلاب وطالبات كلية التربية بجامعة شقراء، وبلغت العينة 190 طالبا وطالبة، وباستخدام المنهج الوصفي. نتائج الدراسة: عدم وجودفروق ذات دلالة إحصائية متعلقة بإجابات أفراد العينة على المحور الأول، ترتبط بالنوع أو التخصص أو المعدل التراكمي.

الدراسة الرابعة:

دراسة الهيف والعنزي 2018 بعنوان: الجرائم المعلوماتية: أنواعها وخطورتها

هدفت الدراسة إلى التعرف على أنواع الجرائم المعلوماتية وخطورتها، وبلغت العينة 250 طالبة، وباستخدام المنهج الوصفي ولاستبانه، توصلت الدراسة إلى أهم نتائج: أن هناك دراية بوجود جرائم معلوماتية ونظام لمكافحتها مع عدم معرفة كيف تتم مكافحة الجرائم المعلوماتية.

8. المقاربة النظرية:

نظرية الضبط الاجتماعي:

تعد نظريات الضبط الاجتماعي من المقاربات الهامة والحاسمة في السياق السوسيولوجي حيث عمدت إلى تفسير السلوكيات الإجرامية والعنيفة على أنها استجابة طبيعية للبناء الاجتماعي، كما أن هذه النظرية تفسر الجريمة والعنف من خلال القيود المتمثلة في المعايير الاجتماعية. ومن جهة أخرى فإن نظرية الضبط الاجتماعي تدور حول افتراض أساسي مآله أن الدافع للجريمة ولانحراف شيء طبيعي يوجد لدى جميع الأفراد، كما تذهب هذه النظرية إلى أن الطاعة والامتثال هو الذي يجب أن يتعلمه الفرد، وعليه تنظر هذه النظرية إلى أن التدابير الاجتماعية والمتمثلة في الامتثال للمعايير واحترامها هو الشرط الأساسي والضامن للضبط، وغيابه يؤدي إلى الجريمة والانحراف. كما ظهرت أشكاله بشكل مباشر أو غير مباشر

في توجيه سلوك الأفراد وضبط تجمعاتهم وتنظيم قواعد التوافق بين معايير الفرد الذاتية والقيم الاجتماعية، وهناك ثلاثة أنماط من الضبط الاجتماعي:

1 الضبط المباشر: وهو أسلوب ظاهري يشير إلى الروابط التي توضع أمام الفرد مثل القوانين الرسمية التي تحرم أنواعا معينة من السلوك أو صور للعقاب المختلفة.

2 الضبط الغير مباشر: وهو يركز أساسا على الارتباط العاطفي بالوالدين وبأشخاص معينين.

3الضبط الذاتي: وهو يشير إلى الشعور لدى الفرد والذي يعمل على توجيه سلوكه عندما تتدرج القواعد والقوانين في نفس الفرد، تصبح جزء لا يتجزأ منه.[1]

وحسب هذه النظرية فإن احترام المعايير والقيم الاجتماعية هو الشرط الأساسي لعملية الضبط أما السلوك لانحرافي والإجرامي فيفسر بإخفاق المجتمع في تقويم وضبط سلوك الأفراد من أجل احترام المبادئ والمعايير الاجتماعية.

وكما يرى العالم أيرش أنه كلما كانت علاقة الفرد بالمجتمع قوية كلما قلت فرص الانحراف، ولكن ليس بالضرورة، وباختصار تنظر نظرية الضبط الاجتماعي إلى الطبيعة البشرية من خلال الافتراض القائم على أن الجريمة والانحراف أمر طبيعي وسوي فمن خلال وجود نظام أخلاقي قائم وإطار مرجعي تقليدي في المجتمع نجد نظرية الضبط الاجتماعي من خلال المؤسسات الاجتماعية تزيد من قوة الرابطة التي تربط الأفراد بالنظام الأخلاقي كما أنها تضعف أيضا وتسمح هذه الرابطة الضعيفة بصورة آلية ازدياد الجريمة والانحراف.[2]

[1] محمد بن عودة، النظريات المعاصرة للجريمة والانحراف، جامعة الجيلالي بونعامة خميس مليانة، 2016-2017، ص08

[2] محمد بن عودة، نفس المرجع السابق

خلاصة الفصل:

تم في هذا الفصل إبراز الإطار المنهجي العام الذي سنلتزم به في البحث حيث حاولنا من خلال هذا الفصل إعطاء نظرة عامة حول الوعي الأمني وعلاقته بالجريمة المعلوماتية في المجتمع الجزائري ومحاولة الالتزام وتوضيح الجوانب الضرورة المراد دراستها انطلاقا من الإشكالية وصياغة التساؤلات إلى تحديد المفاهيم، وكذا توضيح الأهداف الأساسية من خلال دراستنا وصولا إلى المقاربة النظرية.

الفصل الثاني

الفصل الثاني : الجريمة المعلوماتية

تمهيد:

تشير الجريمة المعلوماتية إلى الأنشطة غير القانونية التي تتم باستخدام التكنولوجيا الرقمية والشبكات الإلكترونية وتتنوع هذه الجرائم لتشمل اختراق الأنظمة، سرقة البيانات الشخصية والمالية ونشر البرمجيات الخبيثة والتصيد الاحتيالي، مع ازدياد الاعتماد على التكنولوجيا في الحياة اليومية، أصبحت الجرائم المعلوماتية تشكل تهديدا كبيرا للأفراد والمؤسسات والحكومات مما يتطلب تطوير وسائل حمايةو تعاون لمكافحتها والتصدي لها بفعالية.

المبحث الأول: مفهوم الجريمة المعلوماتية

المطلب الأول: تعريفها

مع دخول الحاسوب والإنترنت الى مجتمعنا وفي كافة جوانب حياتنا بدأ ظهور نوع جديد من الجرائم تسمى الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها حيث نقوم بتعريفها قانونيا وفقهيا

أولا: التعريف الفقهي

فمن التعريفات التي تستند الى موضوع الجريمة او أحيانا إلى أنماط السلوك الإجرامي تعريف الأستاذ ROSENBALT بأنه نشاط غير مشروع موجه لنسخ او تغير أو حذف والوصول إلى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقة او كما عرفها الفقيه سولارز أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات.[1]

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة فان أصحابها ينطلقون من ان الجرائم المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ومن هذه التعريفات:

تعريف الأستاذ جون فور ستر فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ويعرفها نادمان بانها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب.

ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية اي جريمة لفاعلها معرفة فنية بالحسابات تمكن من ارتكابها.

[1] هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية،القاهرة 1992،ص 120

كما عرفها الأستاذ دافيد تمسن أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي. [1]

ثانيا: تعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في النص المادة 02_الفقرة_أ–من القانون رقم 09–04 المؤرخ في 05 اوت2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول بان الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات او اي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية.[2]

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية فانه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بانها كل السلوكيات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها او محلا لوقوعها أي الجرائم التي ترتكب في البيئة الرقمية الالكترونية.[3]

المطلب الثاني: تاريخها

تعد الجريمة المعلوماتية من الجرائم المستحدثة فقد تزامن ظهورها مع ظهور أعظم اختراع في العالم الحديث وهو الحاسب الالي والانترنت وهي إفراز لما نعيشه من ثورة معلوماتية فرغم حداثتها إلا إنها تشكل عائقا حقيقيا لاقتصاديات الدول وخصوصيات الأفراد حيث تتميز على ثلاث مراحل هي:

[1] هشام محمد فريد رستم، عقوبات و مخاطر جرائم معلوماتية، دار النهضة العربية ، القاهرة 2000، ص 20

[2] خالد ممدوح ، أمن الجريمة الالكترونية ، الدار الجامعة إسكندرية 2008، ص 41

[3] طارق إبراهيم دسوقي عطية، الأمن ألمعلوماتي، دار جامعة جديدة 2015، ص153

المرحلة الأولى: من شيوع استخدام الحواسيب في الستينات على السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر.

وتوافقت هذه النقاشات مع التساؤل حول ما اذا كانت جرائم بالمعنى القانوني ام مجرد سلوكيات غير اخلاقية في بيئة او مهنة الحوسبة ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت العديد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية وبدأ الحديث عنها بوصفها ظاهرة إجرامية لمجرد سلوكيات مرفوضة.

المرحلة الثانية: في الثمانينات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات والبرامج.

المرحلة الثالثة: مع انتشار الانترنت في التسعينيات شهدت تناميا هائلا في حقل الجرائم المعلوماتية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ماأحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت انماط جديدة إنكار الخدمة التي على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها الى ملايين المستخدمين في ذات الوقت وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على ثارة الاحقاد او المساس بكرامة واعتبار الاشخاص او المروجة لمواد غير قانونية او غير المشروعة.

وكانت حادثة القرصنة على موقع شركة ياهو عام 2000 من ابرز الحوادث حيث أدت الى توقف الموقع لعدة ساعات.[1]

[1] هشام بشير،2012، الآليات الدولية لمكافحة الجريمة الالكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية

وقد ظهرت الجرائم المعلوماتية لأول مرة بشكل مكثف في المجتمعات الغربية كأمريكا وما جاورها، وذلك لأن هذه التقنية وجدت في الأساس لديهم في معامل وزارة الدفاع الأمريكية، وكان من الطبيعي وجود تجاوزات ومخالفات جسيمة من قبل مستخدمي الانترنت لدى هذه الوزارات الحكومية من الفنيين والمهندسين والمؤتمنين على أجهزة الحاسب، ومما ساعد على انتشار هذا النوع من الجرائم واستفحال خطرها أول الأمر، عدم وجد القوانين التي تجرم الاعتداء على المعلومات والبيانات، وحتى لو فرض وجود هذه القوانين، فإن صعوبة الكشف عن هذه الجرائم وصعوبة ملاحقة فاعليها، أغرى الكثيرين بخوض غمار هذا الفن من فنون الإجرام. [1]

المبحث الثاني: الجريمة المعلوماتية ومظاهرها.

المطلب الأول : أسباب الجريمة المعلوماتية

أسباب الجرائم المعلوماتية متعددة وتشمل:

الأسباب الاقتصادية: تتمثل في الربح المالي ويقوم البعض بارتكاب الجرائم المعلوماتية لتحقيق مكاسب مالية مثل الاحتيال المالي وسرقة الهوية والابتزاز.

البطالة والفقر يمكن أن تدفع الظروف الاقتصادية السيئة بعض الأفراد إلى اللجوء للجرائم المعلوماتية كوسيلة للحصول على المال حيث يجدون في الأنشطة الإجرامية الإلكترونية فرصة لتحقيق دخل مادي سريع.

الأسباب الاجتماعية: البحث عن الاعتراف والشهرة بعض الأفراد وخاصة الهاكرز الشباب يقومون بارتكاب الجرائم المعلوماتية ليظهروا مهاراتهم التقنية ويكسبوا الاعتراف في المجتمعات الالكترونية.

[1]، دراسة مقارنة في التشريعات العربية و الأجنبية ، الرياض ،2014 ، ص 09 أيمن عبد الله فكري ، الجرائم المعلوماتية

الانتقام والكراهية الدوافع الشخصية مثل الغضب الانتقام من فرد معين أو حتى الدوافع السياسية يمكن أن تدفع الأفراد للقيام بالجرائم معلوماتية.[1]

الأسباب التقنية: نقاط الضعف في الأنظمة والثغرات الأمنية في الأنظمة والشبكة والتطبيقات تعتبر هدفا رئيسيا للمجرمين المعلوماتيين واستخدام البرمجيات غير المحدثة أو الأنظمة غير المؤمنة يسهل عليهم اختراقها.

التطور السريع للتكنولوجيا يمنح المجرمين أدوات وتقنيات جديدة لتنفيذ الهجمات المعلوماتية بطرق أكثر تعقيدا وفعالية.

الأسباب التنظيمية والقانونية: نقص التشريعات والردع القانوني وعدم وجود قوانين صارمة ومحدثة لمكافحة الجرائم المعلوماتية يمكن ان يشجع على انتشارها.

ضعف تطبيق القوانين حتى في الدول التي تمتلك تشريعات قوية قد يكون هناك ضعف في تطبيق هذه القوانين أو نقص في الموارد اللازمة لإنفاذها بفعالية.

الأسباب الثقافية والتعليمية: نقص الوعي الأمني العديد من الأفراد والمؤسسات لا يملكون الوعي الكافي حول أهمية الأمن السيبراني وطرق حماية المعلومات الشخصية والمؤسسية هذا الوعي الضعيف يجعلهم أهداف سهلة.

ضعف التعليم التقني: عدم توفر تعليم تقني متقدم ومعرفة كافية بتكنولوجيا المعلومات يمكن أن يؤدي إلى عدم القدرة على فهم التهديدات الالكترونية وكيفية التعامل معها بشكل فعال.

[1]، الجريمة الافتراضية الملتقى الدولي التنظيم القانوني للانترنت و الجريمة الالكترونية ، الجلفة ، الجزائر 2009 دياب البداينة

كل هذه العوامل ولأسباب تتفاعل مع بعضها البعض لتخلق بيئة مواتية لنمو وانتشار الجرائم المعلوماتية. [1]

المطلب الثاني: مظاهر الجريمة المعلوماتية

للجريمة المعلوماتية مظاهر وأساليب يستخدمها المجرمون لتحقيق أهدافهم من بينها:

1. تخريب المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات السجلات الرسمية

2. تزوير المعلومات وتشمل تغيير في المعلومات وتحريفها مثل تغيير علامات الطلاب.

3. انتهاك وتغيير المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

4. انتهاك الخصوصية وذلك بنشر معلومات ذات طبيعة خاصة على الأفراد والدخول لحسابات الأفراد الالكترونية.

5. التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهواتف.

6. التشهير ويشمل استخداما المعلومات الخاصة أو ذات صلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

7. سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.

8. السرقة العلمية للكتب والبحوث العلمية الأكاديمية وخاصة ذات طبيعة تجريبية وتطبيقية.

[1] ذياب الرشيد ، ناصر الصالح،فحص النظرية العامة للجريمة في المملكة العربية السعودية ، المجلد 20، العدد 1 ، ص 141 142

9. الدخول الغير قانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال التخريب.[1]

10 الاحتيال المالي بالبطاقات وهذا ناتجا لاستخدام غير الشرعي للبطاقات والاحتيال المالي ويشمل سرقة الأموال عبر الانترنت وغسيل الأموال الالكتروني

11. التصيد الاحتيالي وتعني استخدام رسائل البريد الالكتروني أو المواقع الوهمية لخداع المستخدمين والحصول على معلومات حساسة مثل كلمات المرور.

12. التشهير وترويج المعلومات الزائفة ونشر الأكاذيب والشائعات لتشويه سمعة الأفراد أو الشركات

13. الاحتيال المالي بالبطاقات وهذا ناتج لاستخدام غبر شرعي للبطاقات

14. البرمجيات الخبيثة وتوزيع المعلومات الزائفة نشر الأكاذيب والشائعات لتشويه سمعة الأفراد أو الشركات

الإرهاب الالكتروني ويقصد به انتهاك المؤسسات والشركات هدفها تكوين جماعات اجرامية.[2]

المبحث الثالث: أثار الجريمة المعلوماتية

المطلب الأول: أثرها على الفرد

الخسارة المالية أو خسارة الدخل:

من أكثر أثار الجرائم المعلوماتية شيوعا على الأفراد الخسارة المالية.غالبا ما يستخدم مجرمو الإنترنت أساليب مختلفة مثل التصيد الاحتيالي والقرصنة والبرامج الضارة للوصول إلى

[1] جابر ضرغام (2017)،جريمة التجسس المعلوماتي دراسة مقارنة ، جمهورية مصر العربية ، المركز العربي للدراسات و البحوث العلمية، ص17

[2] جابر ضرغام (2017)،مرجع سابق

المعلومات المالية للفرد مثل أرقام بطاقات الائتمان وتفاصيل الحساب المصرفي وكلمات المرور يمكن أن يؤدي ذلك إلى خسارة الأموال من خلال المعاملات غير المصرح بها والتي قد يكون من الصعب استردادها.

سرقة الهوية:

سرقة الهوية هي نتيجة مهمة أخرى للجرائم المعلوماتية للأفراد يمكن لمجرمي الانترنت استخدام المعلومات الشخصية المسروقة مثل أرقام الضمان لاجتماعي وأرقام رخص القيادة وتواريخ الميلاد لفتح حسابات جديدة والحصول على قروض وارتكاب أنواع أخرى من الاحتيال باسم الفرد يمكن أن يؤدي ذلك إلى خسارة مالية ومتاعب قانونية وإدارية كبيرة في استعادة هوية الفرد.[1]

الصدمة العاطفية:

بالإضافة إلى الخسارة المالية وسرقة الهوية يمكن أن تسبب الجرائم المعلوماتية صدمة عاطفية غالبا ما يشعر ضحايا الجرائم المعلوماتية بالانتهاك والضعف مما يؤدي إلى الخوف والقلق يمكن أ، يكون لهذا تأثير طويل الأمد على الصحة العقلية للفرد خاصة إذا كان يشعر بالعزلة وغير قادر على طلب المساعدة

فقدان السمعة:

يمكن أن تسبب الجرائم المعلوماتية في الإضرار بسمعة الفرد يمكن لمجرمي الإنترنت استخدام المعلومات المسروقة لنشر محتوى محرج أو ضار عبر الإنترنت مما يؤدي إلى الخوف.[2]

[1] منى شاكر فراج العبسلي، تأثير الجريمة الالكترونية على النواحي الاقتصادية ، كانون أونلاين ،2020،ص 21 20

[2] أبو بكر أحمد همام عبد المجيد ، أثار الجرائم المعلوماتية وسبل مكافحتها ، الوادي 2020 ، ص32

المطلب الثاني: أثرها على المجتمع

الأثر الاقتصادي: يمكن أن يكون للجرائم المعلوماتية تأثيرا كبيرا على الاقتصاد يمكن أن يؤدي إلى خسائر مالية للأفراد والشركات والحكومات يمكن أ، تكلفة إصلاح الأضرار التي لحقت بالأنظمة واستعادة البيانات المفقودة ومنع الهجمات المستقبلية باهظة ويمكن أن يؤثر أيضا على ثقة المستهلك في المعاملات عبر الإنترنت مما يقلل من مبيعات الأعمال وإيراداتها بالإضافة إلى ذلك يمكن أن تؤدي الجرائم المعلوماتية إلى فقدان الملكية الفكرية مما يؤثر سلبا على الإبتكار في الصناعة والقدرة التنافسية

مخاوف الأمن القومي: يمكن أن تشكل الجرائم المعلوماتية تهديدا خطيرا للأمن القومي يمكن أن تؤدي الهجمات على الشبكات الحكومية والعسكرية إلى تعريض المعلومات الحساسة للخطر وتعطيل العمليات يمكن لمجرمي الإنترنت أيضا استخدام التكنولوجيا للانخراط في التجسس وسرقة أسرار الدولة وتعطيل البنية التحتية الحيوية مثل شبكات الطاقة وأنظمة النقل بالإضافة إلى ذلك بمكن استخدام الجرائم المعلوماتية لأغراض سياسية مما يؤدي إلى اضطرابات اجتماعية وسياسية.

التأثير على الرعاية الصحية والسلامة العامة: يمكن أن يكون للجرائم المعلوماتية تأثير كبير على الرعاية الصحية والسلامة العامة يمكن أن تؤدي الهجمات على أنظمة الرعاية الصحية إلى تعريض بيانات المرضى الحساسة للخطر وتعطيل الخدمات الطبية مما قد يؤدي إلى عواقب تهدد الحياة بالإضافة إلى ذلك فإن الهجمات على البنية التحتية الحيوية مثل أنظمة الاستجابة للطوارئ وشيكات النقل يمكن أن تعرض السلامة العامة للخطر يمكن لمجرمي الانترنت أيضا استخدام التكنولوجيا لارتكاب سرقة الهوية مما قد يؤدي إلأى إلحاق الضرر بالأفراد ماليا.

زيادة التنمر والتحرش عبر الإنترنت: يمكن أن تؤدي الجرائم المعلوماتية إلأى زيادة التنمر والتحرش عبر الانترنت يمكن لمجرمي الانترنت استخدام التكنولوجيا لاستهداف الأفراد

والمجموعات ونشر محتوى ضار ورسائل مضايقة يمكن أن يؤدي ذلك إلى تضرر عاطفي ونفسي وإلحاق الضرر بالصحة العقلية مما يؤدي إلى الاكتئاب والقلق بالإضافة إلى ذلك يمكن للجرائم المعلوماتية أن تنشر معلومات مضللة مما قد يكون له عواقب اجتماعية وسياسية خطيرة.[1]

التلاعب بوسائل التواصل الاجتماعي: التلاعب بوسائل التواصل الاجتماعي هو شكل من أشكال الجرائم المعلوماتية التي تنطوي على استخدام منصات وسائل التواصل الاجتماعي للتأثير على الأفراد أو المجموعات أو خداعهم أو التلاعب بهم لتحقيق مكاسب سياسية أو مالية أو شخصية، يمكن أن يتخذ ذلك أشكالا عديدة بما في ذلك نشر معلومات كاذبة وإنشاء ملفات تعريف أو شخصيات مزيفة واستخدام الروبوتات أو الحسابات الآلية لتضخيم الرسائل.

يمكن أن يكون يكون تأثير التلاعب بوسائل التواصل الاجتماعي على المجتمع كبيرا لأنه يمكن أن يقوض سلامة العمليات الديمقراطية ويعزز إيديولوجيات المتطرفة ويؤدي إلى تأكل ثقة الجمهور في المؤسسات ومصادر المعلومات.[2]

[1] هلال نصار، إنعكاسات الجرائم الالكترونية على المجتمع ورؤية قانونية ، 2022، ص 06

[2] هلال نصار، مرجع سابق تم ذكره

خلاصة الفصل:

قمنا في هذا الفصل بإبراز مفهوم الجريمة المعلوماتية والتطور التاريخي لها وإظهار أسبابها والمظاهر التي تخلفها وإظهار الآثار التي تخلفها على الفرد والمجتمع.

الفصل الثالث

الفصل الثالث: الوعي الأمني

تمهيد:

الوعي الأمني يعتبر من الركائز الأساسية للحفاظ على سلامة الأفراد والمجتمعات في مواجهة التهديدات الأمنية المتنوعة.

يشمل الوعي الأمني إدراك الأفراد للمخاطر المحتملة، وفهم الإجراءات الوقائية اللازمة للتعامل معها، والتعرف على السلوكيات والتدابير التي تساهم في تعزيز الوعي الأمني وتعزيز الأمن الشخصي والجماعي، يتطلب الوعي الأمني تضافر جهود متعددة تشمل التعليم والتدريب المستمر لتعزيز قدرة الأفراد على التعرف على التهديدات والاستجابة لها بفعالية مما يسهم في خلق بيئة أكثر أمانا واستقرارا.

المبحث الأول: الوعي الأمني وأهميته

المطلب الأول: مفهوم الوعي الأمني

تعددت الاتجاهات في تحديد معنى الوعي الأمني حيث يرى البعض أن الوعي الأمني يتحقق بإدراك الفرد بالمبادئ والأحكام الأمنية وما يترتب عليها من ممارسة للقواعد الأمنية ويذهب البعض الأخر إلى أن الوعي الأمني يتعلق بالجانب الوجداني لدى الفرد والمتمثل في الشعور بالخطر والرغبة في الشعور بالأمان وفيما يلي أهم التعريفات التي تناولت الوعي الأمني في كل من الاتجاهين:

أ _ الوعي الأمني باعتباره إدراك للمبادئ والقواعد الأمنية:

يرى أصحاب الاتجاه الأول أ، الوعي الأمني هو مصطلح مستمد من علم النفس ويقصد به إحدى العمليات الذهنية التي تعطى الإنسان القدرة على التبصر بالمعلومات الأمنية ومعرفة نتائج ما يقدم عليه من أفعال إرادية والبحث المستمر حول مالا يعرفه عن هذه النتائج حتى يصل إلى تحديدها وذلك عن طريق ربط ما تعلمه في الماضي بوقائع الحاضر ويمد من خلال ذلك نظرة إلى المستقبل فيحوز بذلك على التنبؤ التقريبي بالأمور . [1] .

كما يعرف بأنه عملية تستهدف نشر المعارف والحقائق بقصد تغيير أو تعديل أو تثبيت اتجاهات الفرد أو الجماعة نحو جدث من الأحداث أو ظاهرة من الظواهر ومن ثم مساعدتهم على التفاعل معها بموضوعية وفي نفس الوقت تقوم بتوجيههم إلى أفضل أساليب الوقاية من التحديات والمخاطر المحيطة بهم لمنعها والتقليل من أثارها السلبية. [2]

كما يمكن تعريفه بأنه إدراك الفرد لذاته وللظروف الأمنية المحيطة به وتكوين اتجاه إيجابي نحو الموضوعات الأمنية العامة بالمجتمع.

---

[1] إبراهيم عبد الرحمن، دور الشرطة في مجال تنمية الوعي الأمني لدى الجماهير، كلية الدراسات العليا ،2003 ، ص 05

[2] تركي بن عبد الله ، تصور استراتيجي لتنمية الوعي الأمني للتعامل مع الآخرين ، دراسة الحالة، السعودية 2021 ، ص 14

ويذكر الصالحي أن الوعي الأمني يقصد به توعية الناس بالأنظمة والقوانين لخلق وعي جديد فهو يمثل كافة الجهود التي تبذل في سبيل خلق الوعي في ذهن المواطن.

ويعرف بأنه تثقيف المؤسسات للمواطنين حول السياسات والإجراءات المؤسسية ليمكنهم اكتشاف التهديدات الأمنية التي تواجههم.

ومن التعريفات السابقة يمكن استنتاج ما يلي:

-الوعي عملية ذهنية يمكن تنميتها.

- أن وعي الفرد مكتسب ويمكن تنميته، ويرتبط بما يستمده الفرد من خلال خبرته الشخصية وخبرات الآخرين من حوله.

-الوعي الأمني له جانب عقلي يعكس تصور الفرد لذاته وأهمية سيادة الأمن على المواقف الاجتماعية والظروف المحيطة به في المجتمع وتعلم الفرد لطرق الوقاية من الجريمة بطرق وأساليب تكفل له ولذويه الحماية والأمن.

-الوعي الأمني يتطلب إدراك أهمية المشاركة مع الآخرين في اتخاذ موقف موحد ضد العبث بالأمن والإخلال به وتنمية روح المشاركة مما يولد لدى الفرد سلوكا اجتماعيا مرغوبا.

-للمؤسسات التربوية دور مهم في التوعية الأمنية التي تساعد المواطنين على الوعي بالتهديدات والمخاطر المحتملة. [1]

[1] ألصالحي، عبد المحس، الوعي الأمني ودوره في حياتنا اليومية، الرياض ، مطابع العصر 2005، ص 12

ب-الوعي الأمني باعتباره حالة وجدانية:

يرى أصحاب هذا الاتجاه أن الوعي الأمني هو: حالة وجدانية تجعل الشخص يستشعر ما حوله من مصادر الخطر والتهديد المحتملة، مما يدفع به ألأذى اتخاذ وسائل وبدائل للسلامة منها، وتقليل مخاطرها وهذا لا يعني أنه يتنافى مع الشعور بالأمن ولكن ذلك الشعور أو التصور موحى بأمر مهدد للأمن بناءا على معطيات موضوعية خاصة.

ويركز هذا التعريف على الحالة الوجدانية للإنسان التي تدفعه إلى البحث عن المعلومات التي تساعده على الحفاظ على أمنه وتوجه سلوكه. وتنمية الوعي الأمني بهذا المعنى، يعني إمداد الفرد بالمعلومات الأمنية التي تساعده على تغيير اتجاهاته وتوجيه سلوكه نحو استشعار ما قد يعرضه للخطر واتخاذ الإجراءات اللازمة للتعامل مع المخاطر التي تواجه أمنه الشخصي وأمن المجتمع بوجه عام.

والوعي الأمني بهذا المعنى يؤسس على ثلاثة جوانب:

1. الجانب المعرفي والمتمثل في إمداد الفرد بالمعلومات الأمنية.

2. الجانب الوجداني والمتمثل في تغيير اتجاهاته واستشعار الخطر.

3. الجانب السلوكي والمتمثل في اتخاذه للإجراءات الوقائية والتعامل مع المخاطر التي تواجهه.[1]

المطلب الثاني: أهمية الوعي الأمني

شكل الأمن محورا أساسيا في حياة الإنسان منذ القدم فكل الآثار التاريخية القديمة تظهر اهتمام الإنسان بالأمن ووضعه قواعد للسلامة والبحث عن وسائل تساعده على الحفاظ على حياته وتطورت هذه القواعد والوسائل مع تطور المجتمعات وما ترتب على ذلك من تعقيدات فلم يعد

[1] تركي بن عبد الله، تصور استراتيجي لتنمية الوعي الأمني للتعامل مع الآخرين ، دراسة الحالة ، كلية العلوم الإستراتيجية، السعودية، 2021،ص7

يقتصر الأمن في العصر الحديث على الحفاظ على بقاء الإنسان، بل امتد ليشمل العديد من المجالات الأمنية المرتبطة بالتطورات الاجتماعية والاقتصادية والسياسية مثل الأمن الفكري، السياسي، والاجتماعي، أمن المعلومات.

ويتكون الوعي الأمني لدى الإنسان من حاجته للشعور بالأمن والتي تدفعه إلى الدأب في السعي لاستكشاف البيئة المحيطة به والتعرف عليها والتفريق بين النافع والضار منها، ثم الوصول بعد ذلك إلى إشباع حاجته الغريزية للأمن.

و يعتبر الوعي الأمني من أهم الأساليب الوقائية لمواجهة الجريمة والذي انتهجته العديد من الدول مثل هولندا فرنسا للحفاظ على أمنها وتقليل معدل الجريمة وذلك من خلال إمداد المواطنين بمعارف ومعلومات تشمل مبادئ الحفاظ على أمنهم وحثهم على تطبيقها.

كما تعد تنمية الوعي الأمني أسلوبا وقائيا يجنب المجتمع ما يلحقه من تبعات اجتماعية واقتصادية ومعنوية للجريمة يجب أ، تعمل الدولة على تنميته وتطويره بما يخدم مصلحة الأمن والاستقرار.

ويؤدي عدم وجود الوعي الأمني بشكل عام إلى ممارسة سلوكيات أو أ،شطة تقود الفرد لتهديد أمنه الشخصي وأمن المجتمع فوعي المواطن بالقانون وتطبيقه له يقلل كثيرا من نسبة وقوع الجرائم كما أنه السبيل لحثهم على التعاون مع الجهات الأمنية.

وفي ضوء ما سبق يمكن تحديد أهمية الوعي الأمني للفرد والمجتمع في ما يلي:

1-أهمية الوعي الأمني للفرد:

-الحد من فرص وقوع الفرد تحت طائلة القانون.

- الحد من المخاطر والمشكلات الأمنية التي قد يقع فيها الفرد وتعرضه للخطر.

– الإدراك المناسب بكافة تدابير الوقائية التي تقي الفرد من الجريمة وتحرضه على عدم الوقوع فريسة لها.

–القدرة على تحديد أوجه التعاون مع الأجهزة الأمنية في مجال الإبلاغ عم الجرائم في حال حدوثها.

2– أهمية الوعي الأمني للمجتمع:

– يعمل الوعي الأمني بوجه عام على التقليل من الخسائر البشرية زوالقتصادية الناتجة عن حوادث الجرائم.

–يحد الوعي الأمني من المشكلات الأمنية والتي تسبب الجرائم والانحراف مثل تعاطي المخدرات والقتل والسرقة والخطف وغيرها وكذلك سرعة الإبلاغ عن الجرائم أو الظواهر المنذرة بقرب حدوثها فوعي المواطنين هو السبيل لتعاونهم مع الشرطة كما أن وعي المواطن بالقانون وتطبيقه له يقلل من نسبة الجريمة.

– يحد الوعب الأمني من عدد الجرائم المستحدثة التي تحدث من خلال الانترنت مثل سرقة المعلومات الشخصية أ, الحسابات البنكية وغيرها.

3–أهمية الوعي الأمني على المستوى الدولي:

يساعد الوعي الأمني على تضافر الجهود أمام كافة المهددات للأمن الدولي والتعامل معها من خلا موجهة الإرهاب وتفهم الجميع لما تقوم به الدول والمنظمات الأمنية العالمية من جهود وعدم الانسياق خلف الشائعات والأخبار والمعلومات المغلوطة والتي يتم تداولها عبر الانترنت. وبهذا تظهر أهمية الوعي الأمني في منع الجريمة أو التقليل من فرص حدوثها سواء على المستوى الدولي أو العالمي.

وفي ضوء ماسبق يمكن تحديد أهمية الوعي الأمني باعتباره جانب وقائي للفرد والمجتمع والعالم بأسره من خلال تدريب المواطنين على اتخاذ الإجراءات الوقائية والتي تقلل من وقوع الجرائم وكذلك كجانب علاجي يظهر في السلوك التلقائي من المواطنين لمواجهة الجريمة.

المبحث الثاني: مؤسسات التنشئة الاجتماعية والوعي الأمني

المطلب الأول: مؤسسات التنشئة الاجتماعية والوعي الأمني

تعريف التنشئة الاجتماعية:

قبل تحديد معنى التنشئة الاجتماعية، لابد من تحديد مفهوم التنشئة بصفة عامة:

-التنشئة لغة: جاء في لسان العرب لابن منظور كلمة التنشئة من الفعل نشأ، ينشأ، نشوءا ونشاء بمعنى ربا وشب.[1]

أما التنشئة الاجتماعية، فتعرف بأنها: عملية التفاعل التي يتم من خلالها تكييف الفرد مع بيئته الاجتماعية وتشكيليه ليمثل معايير مجتمعه، وهذه العملية تقوم أساسا على نقل التراث الثقافي والاجتماعي.

بمعنى أن التنشئة الاجتماعية تعمل على نقل الموروث الثقافي والحضاري للمجتمع كأساس لتكييف الفرد مع المجتمع.

وتعرف التنشئة الاجتماعية أيضا بأنها: العملية التي يتم من خلالها وبواسطتها تعليم الفرد الامتثال لمطالب المجتمع والاندماج في ثقافته، والخضوع لالتزاماته ومجاراة الآخرين بوجه عام.[2]

[1]ابن منظور، ج.د (1978)، لسان العرب بيروت، دار صادر، ص 25

[2]شريف، ع (2004)، التنشئة الاجتماعية للطفل في عصر العولمة ، مصر ،دار الفكر العربي، ص 08

ويعرفها بارسونز بأنها: عملية تعليم تعتمد على التلقين والمحاكاة والتوحد مع الأنماط العقابية والعاطفية والأخلاقية عند الطفل الراشد، وهي عملية تهدف إلى إدماج عناصر الثقافة في نسق الشخصية، وهي عملية مستمرة لانهاية لها.[1]

بناءا على ما سبق يمكن تعريف التنشئة الاجتماعية بأنها الاهتمام بالإنسان وتطوره في محيطه الاجتماعي وبيئته اليومية، حيث تجعله قادرا على التفاعل ولاندماج بسهولة مع أفراد المجتمع من خلال اكتسابه الحكم الخلقي والضبط الذاتي لهم حتى يصبحوا أعضاء راشدين ومسئولين في مجتمعهم.

تلعب مؤسسات التنشئة الاجتماعية دورا محوريا في تشكيل الوعي الأمني للأفراد يمكن توضيح العلاقة بينهما كما يلي:

1.الأسرة: تعتبر الأسرة أولى مؤسسات التنشئة الاجتماعية التي يتعرض لها الفرد من خلالها يتعلم الأطفال القيم والمبادئ الأساسية بما في ذلك مفاهيم الأمن والسلامة، الأهل يلعبون دورا كبيرا في توعية أبنائهم بأهمية الحذر وتأمين المنزل وأسس السلوك الاجتماعي الآمن.

فأهمية الأسرة في التنشئة الاجتماعية هي أن:

الأسرة وما تشمل عليه من أفراد هي المكان الأول الذي يتم فيه الاتصال الاجتماعي الذي يمارسه الطفل مع بداية سنوات حياته مما ينعكس على نموه الاجتماعي فيما بعد.

إن القيم والتقاليد والاتجاهات والعادات تمر بعملية تنقية من خلال الآباء لتأخذ طريقها إلى الأبناء بصورة مصفاة وأكثر خصوصية.

الأسرة هي المكان الوحيد في مرحلة الطفولة المبكرة للتربية المقصودة المصحوبة بتعلم اللغات ومهارات التعبير.

[1] دياب،ف (1978)، نمو الطفل وتنشئته بين الأسرة ودور الحضانة، مصر، مكتبة النهضة العربية، ص 114

2. **المدرسة:** المدرسة تعزز ما تعلمه الطفل في الأسرة وتوسع معرفته بالأمن من خلال المناهج الدراسية ويمكن للمدارس تنظيم ورش عمل ومحاضرات حول الوعي الأمني مثل كيفية التعامل مع الطوارئ والكوارث وأهمية الالتزام بالقوانين.[1]

3. وسائل الإعلام: تلعب وسائل دورا كبيرا في تشكيل الوعي الأمني من خلال نشر الأخبار والتقارير والتحقيقات التي تركز على القضايا الأمنية، البرامج التوعية والأفلام الوثائقية تسهم في نشر الوعي بين الجمهور حول مختلف التهديدات الأمنية وكيفية مواجهتها.

ويتمثل أثر الإعلام في التنشئة الاجتماعية فيما يلي:

-نشر التعليم تساعد وسائل الإعلام في تيسير سبل التعلم والتعليم.

-الإسهام في حل المشكلات التي تعترض الحضارة الإنسانية وفي مقدمتها الأمية.

-غرس القيم والمفاهيم والمعتقدات المناسبة للنفوس.

-الترقية وهو ضروري لمنح الراحة التي تمكن البشر من مواجهة متطلبات الحياة.

وعليه تلعب وسائل الإعلام دورا بارزا في تنشئة الفرد من خلال ما تقدمه من معلومات وحقائق وأخبار وآراء.

4. المؤسسات الدينية: تقدم المؤسسات الدينية تعاليم وإرشادات تعزز من السلوكيات الآمنة والمسئولة غالبا ما تدعو القيم الدينية إلى احترام القانون والمحافظة على الأمن والنظام.

ويتلخص أثر المؤسسات الدينية في التنشئة والوعي الأمني في:

-إمداد الفرد بإطار سلوكي تابع من تعاليم دينية.

[1] أبو جادو، سيكولوجية التنشئة الاجتماعية ، الأردن ، دار المسيرة ، 2006، ص 16

-الدعوة إلى ترجمة التعاليم الدينية إلى أفعال.[1]

5. المجتمع المحلي والجماعات المدنية: التدريب على المهارات الأمنية تقديم ورش عمل مجانية لتعليم المهارات الأمنية الأساسية مثل الإسعافات الأولية والدفاع عن النفس

شبكات الأمان لاجتماعي : إنشاء شبكات دعم مجتمعي تساعد في الإبلاغ عن الأنشطة المشبوهة وتعزيز التعاون الجيران للحفاظ على الأمن المحلي.

6. بيئة العمل: تطبيق معايير الأمان الالتزام بتطبيقها في أماكن العمل بما يشمل توفير معدات السلامة وإجراء تدريبات دورية

ثقافة الأمان تشجيع ثقافة الأمان من خلال سياسات الشركة التي تركز على الوقاية من الحوادث والتعامل الفعال مع المخاطر

7. المؤسسات الحكومية: التشريعات والسياسات وضع تشريعات وسياسات تعزز الوعي الأمني مثل قوانين مكافحة الجريمة وحماية البيانات الشخصية.

المبادرات الحكومية إطلاق مبادرات حكومية تستهدف رفع مستوى الوعي الأمني بين المواطنين مثل برامج الجندي الصغير التي تعلم الأطفال مبادئ الأمن الوطني.

8.التكنولوجيا: تطبيقات الهواتف الذكية تطوير تطبيقات تتيح للمواطنين الوصول إلى معلومات ألأمان والسلامة بسهولة وتقديم خدمات مثل الإبلاغ عن الحوادث والتواصل مع السلطات.

التحليلات الأمنية استخدام البيانات والتحليلات لتحسين الاستجابة للأزمات وتحديد المناطق الأكثر عرضة للمخاطر الأمنية.[2]

[1] زين العابدين درويش ، علم النفس الاجتماعي أسسه و تطبيقاته، دار الفكر العربي ، القاهرة ، مصر ، ص 74

[2] عبد الله بن عباس، علم الاجتماع التربوي، المكتب الجامعي الحديث، الإسكندرية، مصر 2002، ص 257

المطلب الثاني: اختلال التنشئة والوعي الأمني

اختلال التنشئة الاجتماعية بمكن أن يكون له تأثير كبير على الوعي الأمني في المجتمع التنشئة الاجتماعية هي العملية التي يتعلم فيها الأفراد القيم والمعتقدات والسلوكيات الضرورية للاندماج في المجتمع، عندما يحدث اختلال في هذه العملية يمكن أن يؤدي ذلك إلى نتائج سلبية على المستوى الفرد والمجتمع.

التأثيرات على الوعي الأمني:

-الجهل بالمعايير الأمنية:

الأفراد الذين لو يتلقوا تنشئة اجتماعية صحيحة قد يفتقرون الى الفهم الواعي لأهمية المعايير الأمنية والاجراءات الوقائية مما يجعلهم أكثر عرضة للانخراط في سلوكيات تعرضهم والمجتمع للخطر

-التفكك الأسري:

العائلات التي تعاني من اختلالات في التنشئة الاجتماعية غالبا ما تكون غير قادرة على غرس القيم والمبادئ الصحيحة في أبناءها مما يؤدي إلى عدم الاستقرار الاجتماعي وزيادة معدلات الجريمة.[1]

-العزلة الاجتماعية:

الأفراد الذين يعانون من اختلال في التنشئة الاجتماعية قد يجدون صعوبة في التفاعل الاجتماعي والتواصل الفعال مما يؤدي إلى العزلة وانسحاب وهما عاملان يمكن أن يقللا من الوعي والمشاركة في الشؤون الأمنية للمجتمع

[1] جودة بن جابر ، علم النفس الاجتماعي، دار الثقافة، الأردن ، ص 113

-التعرض للأفكار المتطرفة:

غياب التنشئة الاجتماعية السليمة يمكن أن يجعل الأفراد أكثر عرضة للتأثر بالأفكار المتطرفة والمجرمين حيث يبحثون عن الانتماء والتقدير في أماكن غير صحيحة.

كيفية تعزيز التنشئة الاجتماعية السليمة والوعي والأمني:

التعليم والتوعية: إدماج مفاهيم الأمن والسلامة في المناهج الدراسية وتقديم ورش عمل ودورات تدريبية للشباب والكبار لتعزيز فهمهم للقضايا الأمنية.

-تعزيز دور الأسرة:

دعم العائلات من خلال برامج الإرشاد والتوجيه لمساعدتها في غرس القيم والمبادئ السليمة في ابنائها.

توفير مساحات آمنة للتفاعل الاجتماعي:

إنشاء مراكز مجتمعة ونواد رياضية وثقافية تساعد في تعزيز الروابط الاجتماعية وتوفر بيئة آمنة للتعلم والتفاعل.

التعاون بين المؤسسات:

تشجيع التعاون بين المدارس والمؤسسات الأمنية والمجتمعات المحلية لتعزيز الوعي الأمني والعمل المشترك للحفاظ على الأمن والاستقرار من خلال معالجة اختلالات التنشئة الاجتماعية وتعزيز الوعي الأمني، يمكن خلق بيئة أكثر أمانا واستقرارا للجميع.[1]

[1] هرندي.ك. مؤسسات التنشئة الاجتماعية بين الأساليب و العوائق، العائلة و المدرسة، مجلة الحوار الثقافي 02 ، ص 104-103

المبحث الثالث: الوعي الأمني ومكافحة الجريمة المعلوماتية

المطلب الأول: تأثير الوعي الأمني على تقليل الجريمة المعلوماتية

تعتبر الوقاية هي أفضل السبل في مكافحة الجريمة المعلوماتية وذلك من خلال التدابير التي يجب أن تتخذها الدول لمنع الجريمة المعلوماتية والحد منها.

وتكمن الصعوبة الأساسية التي تعترض سلطات البحث والتحري في ميدان الجرائم المعلوماتية أن مرتكبي هذه الجرائم لا يتركون في الغالب الأحيان آثارا تدل على ارتكابهم بهذه الجرائم، إذ تكون المعلومات محفوظة تحت رقم أو رمز سريا أو مشفرة كليا إذ يصعب الدخول إليها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء الجناة، لذا وجب السهر على تكوين المحققين من ضباط الشرطة ورجال النيابة العامة وقضاة التحقيق , بل لابد من خلق وحدات خاصة تكون مهمتها الأساسية هي مراقبة وتتبع الشبكة عن طريق الإبحار فيها ومثل هذه المراقبة القبلية قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية.

ويبرز الدور الوقائي في تنمية الوعي الأمني للمواطنين والوعي الأمني هو وعي المواطنين بحقوقه وواجباته القانونية مما يساعد على دعم برامج الأجهزة والمؤسسات الأمنية للتصدي للجريمة المعلوماتية بأنواعها المختلفة من خلال عمليات الوقاية، ومنها ارتكاب الجريمة، والوعي الأمني عملية مركبة تتضمن معرفة الحقائق وإدراك المصالح المادية والثقافية وغيرها، وعلاقة هذه المصالح بالواقع الاجتماعي والسياسي والثقافي السائد مع تجنب المصالح الذاتية والانحياز إلى مصلحة المجتمع، ويجب على تلك الأجهزة تبني إستراتيجية للتوعية الأمنية للمواطنين.[1]

و يكون تأثير الوعي الأمني على مكافحة الجرائم المعلوماتية أيضا عن طريق:

[1] جابر، ضرغام، (2017). جريمة التجسس المعلوماتي "دراسة مقارنة" ، جمهورية مصر العربية ، المركز العربي للدراسات والبحوث العلمية، ص 23

1. زيادة الوعي الأمني بالجرائم المعلوماتية والتثقيف بمخاطرها، وتوجيه الأفراد بضرورة المحافظة على معلوماتهم الخاصة وحفظ تلك الخصوصية بكلمات مرور قوية بما يتعلق بمسائلهم الشخصية مثل أرقامهم الوظيفية والحسابات البنكية والبطاقات الائتمانية.

2. سن التشريعات والقوانين التي تتسم بالمرونة والحداثة ومواكبة التطورات التقنية لحماية الفرد والمجتمع من الجرائم المعلوماتية.

3. تخصيص مؤسسات خدمية في المجتمع يسهل الوصول إليها أرقام تواصل سهلة للإبلاغ عن الجرائم المعلوماتية.

4. توظيف التقنيات الرقمية للمساهمة في كشف هوية منفذي الجريمة المعلوماتية.

5. إصدار السياسات المنظمة لعقوبات تطبق على منفذي الجرائم المعلوماتية.[1]

المطلب الثاني: مكافحة الجريمة المعلوماتية في التشريع الجزائري

أمام الحركة التشريعية الدولية في مجال مكافحة الجرائم المعلوماتية، كان على المشرع الجزائري الاستجابة لمثل هذه التحديات لهذا سنتطرق في هذا المطلب للحماية التي كلفها المشرع الجزائري لمعطيات الحاسب الآلي من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذلك من خلال نصوص المعالجة الآلية للمعطيات وأيضا من خلال نصوص قانون الملكية الفكرية.

[1] محمد عبد الله أبو بكر، موسوعة جرائم معلوماتية، المكتب العربي الحديث، الإسكندرية، 2011، ص 10

أولا: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحتها.

بعد تفاقم الاعتداءات على معطيات الكمبيوتر نتيجة ضعف الحماية الفنية، تدخل المشرع الجزائري بموجب القانون رقم 09-04 الخاص بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الأعلام والاتصال ومكافحتها، إذ أجازت المادة 03 منه مراقبة الاتصالات الالكترونية لكن هذه المراقبة ليست مطلقة، حيث قيدتها المادة 04 من نفس القانون حيث حددت الحالات التي يلجأ فيها للمراقبة الالكترونية مع الحصول على إذن مكتوب من السلطة القضائية وحددت القانون السالف الذكر بعض القواعد الاجرائية كالتفتيش والحجز في المواد 05-06، كما قام هذا القانون بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته وكذا تفعيل المراقبة عن بعد من خلال المساعدة القضائية الدولية بمساعدة الهيئة السالف الذكر، في المواد 16-17- 18 منه.[1]

ثانيا: الحماية في قانون العقوبات.

قام المشرع الجزائري بتعديل قانون العقوبات، حيث تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 156/66 بالقسم السابع مكرر معنون ب (المساس بأنظمة المعالجة الآلية للمعطيات) من المادة 394 مكرر إلى المادة 394 مكرر 7، وقد عالجها المشرع الجزائري من خلال عدة أفعال مجرمة، هي كالآتي:

_ الدخول للمنظومات المعلوماتية عن طريق الغش: فقد اعتبرها جريمة بسيطة قرر لها عقوبة الحبس من 3 أشهر إلى سنة وبغرامة 50.000 إ إلى 100.000دج، وتضاعف العقوبة إن كان هنالك حذف أو تعديل، وإن كان هناك تخريب لنظام اشتغال المنظومة يعاقب الفاعل من

[1]قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

06 أشهر إلى سنتين والغرامة من 50.000 إلى 150.000دج [1]، أما إن أزال أو عدل المعطيات التي يتضمنها نظام المعالجة الآلية يعاقب الفاعل بالحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من 500.00 إلى 2.000.000.[2]

_ التصرف عمدا في المعطيات عن طريق الغش يعاقب الفاعل بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من 1.000.000 إلى 5.000.000 دج.[3]

_ تضاعف العقوبة إن استهدفت الجريمة الدفاع الوطني أو المؤسسات الخاضعة للقانون العام.[4]

_ تضاعف العقوبة المقررة للشخص العادي خمسة مرات إن كان الفاعل شخص معنوي.[5]

_ يعاقب على الشروع، أو المشاركة في الفعل أو المشاركة في اتفاق لتنفيذ الجريمة بنفس العقوبة المقررة للجريمة ذاتها.[6]

ثالثا: الحماية في القوانين الخاصة

هناك بعض القوانين الخاصة التي طرحت حماية من الجرائم المعلوماتية في بعض المجلات:

1_ الحماية في قانون التأمينات: حيث يعاقب هذا الأخير كل من يسلم أو يستلم بهدف الاستعمال غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا، أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني المهني، كما يعاقب كل تعدي على بيانات البطاقة في حد ذاتها وإن كان المعتدي شخص معنوي تضاعف العقوبة خمس مرات المبلغ الأقصى.

[1] المادة 394 مكرر من قانون العقوبات الجزائري
[2] المادة 394 مكرر 1 من قانون العقوبات الجزائري
[3] المادة 394 مكرر 2 من قانون العقوبات الجزائري
[4] المادة 394مكرر 3 من قانون العقوبات الجزائري
[5] المادة 394مكرر 4 من قانون العقوبات الجزائري
[6] المادة 394 مكرر 5 والمادة 394 مكرر 7 من قانون العقوبات الجزائري

2_ الحماية في النصوص الملكية الفكرية:

وتنقسم حقوق الملكية الفكرية بدورها إلى قسمين، حقوق المكية الصناعية التي ترمز إلى المبتكرات الجديدة التي نظمها المشرع بقانون شهادات المخترعين وبراءات الاختراع، ولما كانت برامج المعلوماتية تستعمل للتعامل مع أجهزة الحاسوب حيث لا يشتغل الحاسوب فهي جزء منها، وبذلك من هذه الزاوية تصبح قابلة للبراءة متى توافر شرط الجدة وقابلية الاستغلال الصناعي.[1]

[1]بوعناد فاطمة زهرة ، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول ، 2013، ص65

خلاصة الفصل:

ظاهرة الوعي الأمني من المواضيع التي لازالت محل جدل ونقاش بين التيارات الفكرية والعلمية والتي تعاني منها كافة المجتمعات الإنسانية في الوقت الحالي خاصة في المجتمع الجزائري، وقمنا بتعريفه وذكر أهميته وأهمية مؤسسات التنشئة الاجتماعية بالوعي الأمني وتفشي الجريمة المعلوماتية بكثرة بعد تلاشي واختلال مؤسسات التنشئة الاجتماعية، كما لا ننسى دور الوعي الأمني في مكافحته للجريمة المعلوماتية ودور المشرع الجزائري أيضا.

الفصل الـرابع

الفصل الرابع: الإجراءات المنهجية للدراسة

الإجراءات المنهجية للدراسة

يُعَدّ هذا الفصل من أهم فصول البحث، حيث يركز على الإجراءات المنهجية التي تم اتباعها في الدراسة الميدانية المتعلقة بالوعي الأمني والجريمة المعلوماتية في المجتمع الجزائري.

من خلال هذا الفصل، سنستعرض العينة المستهدفة وأدوات جمع البيانات والطرق التي تم استخدامها لتحليل هذه البيانات. هذا التحليل يهدف إلى فهم أعمق للعوامل التي تؤثر على الوعي الأمني لدى الأفراد وكيفية التعامل مع الجرائم المعلوماتية، وذلك من خلال جداول البيانات والإحصاءات التي ستسهم في تقديم توصيات فعّالة لمكافحة هذه الجرائم.

تم اختيار عينة مكونة من 70 فردًا من مختلف الفئات العمرية والمستويات التعليمية والجغرافية، بهدف الحصول على نتائج دقيقة وشاملة، واستخدم الباحث الاستبيانات كأداة رئيسية لجمع البيانات، والتي تم تصميمها بعناية لتغطية جميع الجوانب المتعلقة بالوعي الأمني والجريمة المعلوماتية.

1جدول رقم (01) يبين توزيع أفراد العينة حسب الفئة العمرية:

الفئة العمرية	ك	%
من 18 21	21	%30
أكثر من 21 سنة	49	%70
المجموع	70	%100

1. تحليل النتائج

الفئات الأكثر تمثيلاً:

– الفئة العمرية الأكثر تمثيلاً في العينة هي الفئة التي تتجاوز 21 سنة، حيث تشكل 70% من إجمالي العينة. هذا يشير إلى أن الأغلبية العظمى من العينة تقع ضمن هذه الفئة العمرية.

العوامل المؤثرة:

– يمكن أن يكون لتوزيع الفئات العمرية داخل العينة تأثير كبير على النتائج النهائية للدراسة، حيث أن الفئات العمرية المختلفة قد تمتلك سلوكيات وأولويات مختلفة فيما يتعلق بالأمان الإلكتروني والوعي بالمخاطر.

سلوك الفئات العمرية:

– من المرجح أن يكون لدى الفئة الأكبر من 21 سنة مستوى أعلى من الخبرة التكنولوجية ومعرفة أكبر بالمخاطر الإلكترونية مقارنة بالفئة الأصغر (18–21 سنة). هذا قد يؤثر على مستوى تعرضهم للمخاطر أو كيفية تعاملهم مع المواقف المتعلقة بالأمان الإلكتروني.

2. التوصيات

برامج التوعية والتدريب:

– للفئة العمرية من 18 إلى 21 سنة:

– ينبغي تصميم برامج توعية تفاعلية وجذابة تناسب اهتمامات هذه الفئة. يمكن استخدام وسائل التواصل الاجتماعي والمنصات الرقمية لجذب انتباههم وتعليمهم حول الأمان الإلكتروني.

– التركيز على تعزيز المعرفة الأساسية بالأمان الإلكتروني وتطوير المهارات اللازمة لحماية أنفسهم عبر الإنترنت.

– للفئة العمرية أكثر من 21 سنة:

– يمكن تقديم برامج تدريب متقدمة تشمل تحديثات حول أحدث المخاطر الأمنية والتقنيات الجديدة للحماية.

– تشجيعهم على مشاركة تجاربهم ومعرفتهم مع الفئات العمرية الأصغر لتعزيز الوعي الجماعي.

استراتيجيات التنفيذ:

– شراكات مع المؤسسات التعليمية:

– التعاون مع الجامعات والمعاهد لتقديم دورات تدريبية وورش عمل حول الأمان الإلكتروني.

– إشراك الطلاب في مشاريع عملية تمكنهم من تطبيق ما تعلموه في مواقف حقيقية.

– استخدام التكنولوجيا في التعليم:

– استخدام تطبيقات الهاتف المحمول والبرامج التفاعلية لتقديم المعلومات والاختبارات التوعوية بشكل ممتع وجذاب.

– تطوير منصات تعليمية إلكترونية تحتوي على موارد متنوعة يمكن للطلاب الوصول إليها في أي وقت.

3. النتائج

رفع مستوى الوعي:

– من المتوقع أن تؤدي البرامج التوعوية المخصصة إلى زيادة ملحوظة في مستوى الوعي الأمني لدى كلا الفئتين العمريتين، مما يساهم في تقليل نسبة التعرض للاختراقات الإلكترونية.

تغيير السلوكيات:

– على المدى الطويل، يمكن أن تسهم التوعية المستمرة في تغيير سلوكيات المستخدمين ليصبحوا أكثر حرصًا في التعامل مع البيانات الشخصية والمعلومات الحساسة.

تعزيز المهارات:

– تطوير المهارات التكنولوجية للفئة العمرية من 18 إلى 21 سنة قد يساعد في تقليل الفجوة بينهم وبين الفئة الأكبر سنًا، مما يجعلهم أكثر استعدادًا لمواجهة التحديات الإلكترونية.

4. الاستنتاجات

– ضرورة التوعية الموجهة: من الضروري تطوير برامج توعية موجهة تأخذ في الاعتبار الفروقات بين الفئات العمرية. الفئة العمرية الأكبر من 21 سنة تحتاج إلى معلومات متقدمة، بينما الفئة العمرية الأصغر تحتاج إلى أساليب تعليمية جذابة وتفاعلية.

– تأثير الفئات العمرية على النتائج: النتائج تشير إلى أن التركيز على الفئة العمرية الأكبر يمكن أن يكون له تأثير إيجابي كبير نظراً لتفوق عددهم. ومع ذلك، لا يجب إهمال الفئة الأصغر، حيث أن بناء الوعي في سن مبكر يمكن أن يخلق جيلاً أكثر أماناً ووعياً في المستقبل.

– الاهتمام بالتدريب العملي: يجب أن تتضمن برامج التوعية والتدريب عناصر عملية تمكن المتدربين من تطبيق المعرفة النظرية في مواقف حقيقية، مما يعزز الفهم ويزيد من فعالية التعليم.

– التعاون مع المؤسسات التعليمية: التعاون مع المؤسسات التعليمية يمكن أن يسهل الوصول إلى الفئات العمرية المختلفة ويوفر منصة قوية لنشر الوعي الأمني.

وعلى هذا الأساس يمثل الجدول رقم (01) توزيعاً مهماً للفئات العمرية داخل العينة ويشير إلى أن الأغلبية تقع ضمن الفئة الأكبر من 21 سنة. يستدعي هذا تطوير برامج توعية مخصصة لكل فئة عمرية لتعزيز الوعي الأمني وتقليل المخاطر. التركيز على التعليم التفاعلي والتعاون مع المؤسسات التعليمية يمكن أن يعزز من فعالية هذه البرامج ويضمن وصولها لأكبر عدد ممكن من الأفراد.

2.جدول رقم 02 يبين توزيع أفراد العينة حسب الجنس

الجنس	ك	%
ذكر	35	%50
أنثى	35	50%
المجموع	70	100%

1. تحليل النتائج

التوزيع المتساوي:

– يظهر الجدول توزيعًا متساويًا تمامًا بين الذكور والإناث في العينة، حيث أن كل جنس يمثل 50% من إجمالي العينة. هذا التوزيع المتساوي يضمن أن النتائج المستخلصة من العينة يمكن تعميمها بشكل أكثر عدالة على كلا الجنسين.

العوامل المؤثرة:

– توزيع الجنس المتساوي يعزز من دقة التحليل عند دراسة تأثير الجنس على الوعي والممارسات المتعلقة بالأمان الإلكتروني. يمكن أن يساعد ذلك في تحديد ما إذا كانت هناك اختلافات جوهرية بين الذكور والإناث في هذا السياق.

الفروق بين الجنسين:

– يمكن أن يكون هناك فروق في سلوكيات الأمان الإلكتروني بين الذكور والإناث. مثلًا، قد تكون هناك اختلافات في مستوى المعرفة التقنية، أو في نوعية المخاطر التي يتعرضون لها، أو في استجابتهم للمخاطر الإلكترونية.

2. التوصيات

برامج توعية مخصصة:

- للذكور:

- تصميم برامج توعية تستهدف الذكور وتتناول النقاط الضعيفة في سلوكياتهم الإلكترونية. قد تكون هذه البرامج أكثر تركيزًا على الجوانب التقنية وتقديم حلول عملية للتعامل مع التهديدات.

- للإناث:

- تطوير برامج توعية تركز على احتياجات الإناث، مثل كيفية حماية المعلومات الشخصية على وسائل التواصل الاجتماعي وكيفية التعامل مع التهديدات الإلكترونية الخاصة مثل التحرش الإلكتروني.

استراتيجيات التنفيذ:

- ورش عمل مشتركة:

- تنظيم ورش عمل مشتركة لكلا الجنسين لتعزيز تبادل الخبرات والمعرفة. يمكن أن تساهم هذه الورش في تعزيز التعاون والفهم المتبادل بين الجنسين.

- أبحاث إضافية:

- إجراء دراسات إضافية لفهم الفروق الدقيقة بين الجنسين فيما يتعلق بالأمان الإلكتروني، مما يساعد في تطوير برامج توعية أكثر تخصصًا ودقة.

3. النتائج

تحسين الوعي:

– من المتوقع أن تؤدي برامج التوعية المخصصة والمشتركة إلى تحسين الوعي الأمني لدى كلا الجنسين. توفير محتوى مناسب لاحتياجات كل جنس يمكن أن يزيد من فعالية هذه البرامج.

تعزيز المهارات:

– رفع مستوى المهارات والمعرفة التقنية يمكن أن يساعد الذكور والإناث على حد سواء في التعامل مع التهديدات الإلكترونية بشكل أفضل.

تغيير السلوكيات:

– البرامج التوعوية والتدريبية يمكن أن تسهم في تغيير السلوكيات غير الآمنة وتعزيز الممارسات الأمنية الجيدة بين كلا الجنسين.

4. الاستنتاجات

التوزيع المتساوي كعامل قوة:

– التوزيع المتساوي بين الجنسين في العينة يمثل نقطة قوة في الدراسة، حيث يتيح ذلك فهمًا أكثر توازنًا وموضوعية للفروق بين الجنسين في التعامل مع الأمان الإلكتروني.

ضرورة التوعية الموجهة:

– تشير النتائج إلى ضرورة تطوير برامج توعية موجهة تتناسب مع احتياجات وسلوكيات كل جنس لضمان وصول الرسالة بفعالية وتحقيق الأهداف المرجوة.

التعاون والتبادل المعرفي:

– تعزيز التعاون والتبادل المعرفي بين الذكور والإناث يمكن أن يسهم في تحسين مستوى الوعي والمهارات الأمنية لدى كلا الجنسين.

أهمية الأبحاث المستمرة:

– الحاجة إلى أبحاث مستمرة لفهم التطورات والاختلافات في سلوكيات الأمان الإلكتروني بين الجنسين. هذه الأبحاث يمكن أن تقدم رؤى جديدة وتساعد في تطوير استراتيجيات توعية أكثر فعالية.

يوضح الجدول رقم (02) توزيعًا متساويًا بين الذكور والإناث في العينة، مما يتيح فرصة مثالية لفهم الفروق والتشابهات بين الجنسين في مجال الأمان الإلكتروني. من خلال تقديم برامج توعية مخصصة ومشتركة، يمكن تحسين مستوى الوعي الأمني وتعزيز المهارات لدى كلا الجنسين. التعاون المستمر والأبحاث الموجهة يمكن أن تساهم في تطوير استراتيجيات فعالة للتوعية والحماية من التهديدات الإلكترونية.

3جدول رقم 03 يبين توزيع أفراد العينة حسب المستوى الجامعي

المستوى الجامعي	ك	%
ليسانس	36	%51.4
ماستر	34	%48.6
المجموع	70	%100

1. تحليل النتائج

الفئات الأكثر تمثيلاً:

– يظهر الجدول أن الأغلبية النسبية من العينة هم من حملة درجة الليسانس (51.4%)، يليهم حملة درجة الماستر (48.6%). هذه النسب تقارب بعضها، مما يشير إلى تمثيل متوازن نسبيًا للمستويات التعليمية المختلفة.

العوامل المؤثرة:

– المستوى التعليمي يمكن أن يكون له تأثير كبير على الوعي والممارسات المتعلقة بالأمان الإلكتروني. من الممكن أن يكون لدى حملة الماستر مستوى أعلى من المعرفة التقنية مقارنة بحملة الليسانس.

الخبرة والمعرفة:

– من المتوقع أن يمتلك الأفراد الذين يحملون درجة الماستر مستوى أعلى من الخبرة الأكاديمية والمعرفة التقنية، مما قد يجعلهم أكثر قدرة على فهم التهديدات الإلكترونية والتعامل معها بفعالية أكبر.

2. التوصيات

برامج توعية وتدريب متخصصة:

– لحملة الليسانس:

– تصميم برامج توعية تستهدف تعزيز المعرفة الأساسية بالأمان الإلكتروني وتطوير المهارات اللازمة لحماية البيانات الشخصية. يمكن أن تشمل هذه البرامج ورش عمل تفاعلية ودورات تدريبية عبر الإنترنت.

– التركيز على تقديم معلومات حول التهديدات الشائعة وكيفية الوقاية منها بطرق بسيطة وفعالة.

– لحملة الماستر:

– تقديم برامج تدريب متقدمة تغطي أحدث التطورات في مجال الأمان الإلكتروني وتكنولوجيا المعلومات. يمكن أن تشمل هذه البرامج دروسًا متقدمة حول تقنيات الحماية وأدوات الكشف عن الاختراقات.

– تشجيع الأفراد على المشاركة في مؤتمرات وندوات متخصصة لتعزيز معرفتهم والبقاء على اطلاع بأحدث المستجدات في هذا المجال.

استراتيجيات التنفيذ:

– التعاون مع المؤسسات التعليمية:

– الشراكة مع الجامعات والمعاهد العليا لتنظيم ورش عمل ودورات تدريبية متخصصة يمكن أن تستهدف كلا المستويين التعليميين.

– تطوير مناهج تعليمية تشمل مواضيع الأمان الإلكتروني كجزء من البرامج الدراسية للطلاب في جميع المراحل.

– استخدام التكنولوجيا في التعليم:

– استغلال التطبيقات والمنصات الرقمية لتقديم مواد تعليمية تفاعلية ومبتكرة يمكن أن تجذب اهتمام الطلاب وتعزز من فهمهم للمفاهيم الأمنية.

3. النتائج

تحسين الوعي الأمني:

– من المتوقع أن تؤدي البرامج التعليمية المخصصة إلى زيادة ملحوظة في مستوى الوعي الأمني بين جميع المستويات التعليمية. سيصبح الأفراد أكثر قدرة على حماية بياناتهم الشخصية والمهنية.

تعزيز المهارات التقنية:

– تحسين مستوى المهارات التقنية يمكن أن يساعد الأفراد على التعامل مع التهديدات الإلكترونية بفعالية أكبر، مما يقلل من احتمالية التعرض للاختراقات الأمنية.

تقليل الفجوة التعليمية:

– البرامج التوعوية المتخصصة يمكن أن تسهم في تقليل الفجوة المعرفية بين حملة الليسانس وحملة الماستر، مما يضمن توافر مستوى عالٍ من الوعي الأمني لدى الجميع.

4. الاستنتاجات

التنوع في المستوى التعليمي:

– توزيع العينة حسب المستوى التعليمي يظهر توازنًا نسبيًا، مما يعزز من إمكانية تعميم النتائج على جميع المستويات التعليمية.

أهمية التعليم المستمر:

– التعليم المستمر والتدريب المتخصص ضروريان للحفاظ على مستوى عالٍ من الوعي الأمني. يشير التوزيع المتوازن إلى الحاجة إلى استراتيجيات توعية متقدمة تلبي احتياجات جميع المستويات التعليمية.

تأثير التعليم على الأمان الإلكتروني:

– المستوى التعليمي يلعب دورًا مهمًا في تحديد مستوى الوعي الأمني والممارسات الوقائية. يجب أن تكون البرامج التوعوية مصممة بطريقة تتناسب مع الخلفية التعليمية للمستهدفين.

الشراكة مع المؤسسات التعليمية:

– التعاون مع المؤسسات التعليمية يمكن أن يسهم في توفير برامج توعية فعالة ومستدامة، مما يعزز من مستوى الأمان الإلكتروني بشكل عام.

يوضح الجدول رقم (03) توزيعًا متوازنًا نسبيًا بين حملة الليسانس والماستر في العينة، مما يوفر فرصة لفهم تأثير المستوى التعليمي على الوعي والممارسات المتعلقة بالأمان الإلكتروني. من خلال تقديم برامج توعية وتدريب متخصصة، يمكن تحسين مستوى الوعي الأمني وتعزيز المهارات التقنية لدى جميع الأفراد. التعاون مع المؤسسات التعليمية واستخدام التكنولوجيا في التعليم يمثلان استراتيجيات فعالة لتحقيق هذا الهدف

4.جدول رقم 04 يبين توزيع أفراد العينة حسب البيئة الجغرافية

البيئة الجغرافية	ك	%
ريفي	28	%40
حضري	42	%60
المجموع	70	%100

1. تحليل النتائج

التوزيع الأكثر تمثيلاً:

– البيئة الحضرية تمثل الأغلبية في العينة بنسبة 60%، في حين أن البيئة الريفية تمثل 40%. هذا يشير إلى أن معظم أفراد العينة يعيشون في مناطق حضرية.

العوامل المؤثرة:

– البيئة الجغرافية يمكن أن تؤثر بشكل كبير على الوصول إلى التكنولوجيا ومستوى الوعي بالأمان الإلكتروني. من الممكن أن يكون لسكان المناطق الحضرية وصول أكبر إلى الإنترنت والتكنولوجيا المتقدمة مقارنة بسكان المناطق الريفية.

تفاوتات الوصول والمعرفة:

– الأفراد في البيئات الحضرية قد يكون لديهم مستوى أعلى من المعرفة التقنية والوعي بالمخاطر الإلكترونية مقارنة بالأفراد في البيئات الريفية. قد يكون هذا ناتجًا عن توفر موارد تعليمية وتكنولوجية أفضل في المدن.

2. التوصيات

برامج توعية وتدريب مخصصة:

– للبيئة الريفية:

– تصميم برامج توعية تأخذ في الاعتبار محدودية الوصول إلى التكنولوجيا في المناطق الريفية. يمكن تنظيم ورش عمل محلية تستخدم وسائل تكنولوجية بسيطة لزيادة الوعي بالأمان الإلكتروني.

– تقديم محتوى تعليمي يتناول التهديدات الشائعة في البيئات الريفية وكيفية الوقاية منها بطرق سهلة وفعالة.

– للبيئة الحضرية:

– تطوير برامج توعية متقدمة تشمل آخر التطورات في مجال الأمان الإلكتروني. يمكن أن تتضمن هذه البرامج دورات تدريبية عبر الإنترنت وندوات متخصصة.

– تشجيع الأفراد على المشاركة في مجتمعات الأمن الإلكتروني المحلية والافتراضية لتعزيز المعرفة وتبادل الخبرات.

استراتيجيات التنفيذ:

– التعاون مع الهيئات المحلية:

– التعاون مع الهيئات المحلية في المناطق الريفية لتنظيم حملات توعية ومبادرات تعليمية. يمكن استخدام المدارس والمراكز المجتمعية كمنصات لتقديم هذه البرامج.

– الشراكة مع الشركات التقنية في المناطق الحضرية لتقديم ورش عمل ودورات تدريبية مجانية أو منخفضة التكلفة للأفراد المهتمين بتعزيز معرفتهم بالأمان الإلكتروني.

– استخدام التكنولوجيا في التعليم:

– استغلال الهواتف الذكية والتطبيقات التعليمية لتقديم محتوى تفاعلي يمكن الوصول إليه بسهولة من قبل سكان المناطق الريفية والحضرية على حد سواء.

– تطوير منصات تعليمية تحتوي على موارد متنوعة يمكن للطلاب والأفراد في مختلف البيئات الوصول إليها في أي وقت.

3. النتائج

تحسين الوعي الأمني:

من المتوقع أن تؤدي البرامج التعليمية المخصصة إلى زيادة ملحوظة في مستوى الوعي الأمني بين سكان البيئات الريفية والحضرية. سيساعد هذا على تقليل الفجوة في الوعي الأمني بين هاتين الفئتين.

تعزيز المهارات التقنية:

يمكن لرفع مستوى المهارات والمعرفة التقنية أن يساعد الأفراد على التعامل مع التهديدات الإلكترونية بشكل أفضل، مما يقلل من احتمالية التعرض للاختراقات الأمنية.

تقليل الفجوة الجغرافية:

يمكن للبرامج التوعوية المتخصصة أن تسهم في تقليل الفجوة في مستوى الوعي الأمني بين سكان البيئات الريفية والحضرية، مما يضمن توافر مستوى عالٍ من الأمان الإلكتروني للجميع.

4. الاستنتاجات

تأثير البيئة الجغرافية:

تلعب البيئة الجغرافية دورًا مهمًا في تحديد مستوى الوصول إلى التكنولوجيا والوعي الأمني. يشير التوزيع الحالي إلى ضرورة تطوير استراتيجيات توعية تلبي احتياجات سكان كل من البيئات الريفية والحضرية.

ضرورة التوعية الموجهة:

تشير النتائج إلى أهمية تقديم برامج توعية موجهة تتناسب مع الظروف البيئية لكل فئة. سكان المناطق الريفية يحتاجون إلى محتوى تعليمي بسيط وفعّال، بينما سكان المناطق الحضرية يمكنهم الاستفادة من برامج أكثر تقدمًا.

التعاون المجتمعي والمحلي:

يمكن التعاون مع الهيئات المحلية والمجتمعات أن يسهم بشكل كبير في نشر الوعي الأمني وتحسين مستوى الأمان الإلكتروني في جميع البيئات الجغرافية.

التكنولوجيا كأداة تعليمية:

يمكن لاستخدام التكنولوجيا في التعليم أن يعزز من فعالية برامج التوعية ويساعد على الوصول إلى فئات واسعة من السكان في البيئات المختلفة.

يوضح الجدول رقم (04) أن هناك توزيعًا غير متكافئ بين سكان البيئات الريفية والحضرية في العينة، مما يشير إلى تأثير البيئة الجغرافية على الوعي والممارسات المتعلقة بالأمان

الإلكتروني. من خلال تقديم برامج توعية وتدريب مخصصة لكل بيئة جغرافية، يمكن تحسين مستوى الوعي الأمني وتعزيز المهارات التقنية. التعاون مع الهيئات المحلية واستخدام التكنولوجيا في التعليم يمثلان استراتيجيات فعالة لتحقيق هذا الهدف.

الفرضية الأولى

5جدول رقم 05 يبين العلاقة بين الجنس والتعرض للاختراق الالكتروني

الاختراق / الجنس	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
ذكر	7	10%	28	%40	35	%50
أنثى	21	%30	14	%20	35	%50
المجموع	28	%40	42	%60	10	%100

1. تحليل النتائج

الفروق بين الجنسين:

– يظهر الجدول أن نسبة الإناث اللاتي تعرضن للاختراق الإلكتروني (30%) أعلى بشكل ملحوظ من نسبة الذكور الذين تعرضوا للاختراق (10%). في المقابل، نسبة الذكور الذين لم يتعرضوا للاختراق (40%) أعلى من نسبة الإناث اللاتي لم يتعرضن للاختراق (20%).

التفاوتات:

– هذا التفاوت يشير إلى وجود اختلاف في تعرض الجنسين للمخاطر الإلكترونية، مما قد يعكس اختلافات في مستوى الوعي الأمني أو السلوكيات عبر الإنترنت.

العوامل المؤثرة:

– من الممكن أن تكون الإناث أكثر عرضة للاختراقات الإلكترونية بسبب طبيعة استخدامهن للإنترنت أو بسبب قلة وعيهن بالإجراءات الأمنية مقارنة بالذكور.

2. التوصيات

برامج توعية مخصصة:

– للإناث:

– تصميم برامج توعية تستهدف تحسين الوعي الأمني لديهن وتعليمهن كيفية حماية أنفسهن من الاختراقات الإلكترونية. يمكن أن تشمل هذه البرامج ورش عمل تفاعلية ودورات تعليمية عبر الإنترنت.

– التركيز على تعليمهن كيفية التعامل مع التهديدات الشائعة مثل التصيد الاحتيالي والاحتيال الإلكتروني.

– للذكور:

– على الرغم من أن نسبة التعرض للاختراق بينهم أقل، إلا أن التوعية المستمرة مهمة للحفاظ على مستوى الأمان. يمكن تقديم ورش عمل متقدمة تشمل أحدث التقنيات والأساليب لحماية البيانات.

استراتيجيات التنفيذ:

– التعاون مع المنظمات النسائية:

– التعاون مع المنظمات النسائية لنشر الوعي وتقديم الدعم والمعلومات حول كيفية الحماية من التهديدات الإلكترونية.

– تنظيم ندوات وورش عمل موجهة للنساء لزيادة الوعي والمعرفة حول الأمان الإلكتروني.

– استخدام وسائل التواصل الاجتماعي:

– استغلال وسائل التواصل الاجتماعي كمنصة لنشر معلومات توعوية بشكل مستمر حول الأمان الإلكتروني لكل من الذكور والإناث.

– تقديم نصائح يومية ومحتوى تفاعلي يجذب اهتمام المستخدمين ويشجعهم على اتخاذ إجراءات أمنية.

3. النتائج

تحسين الوعي الأمني:

– من المتوقع أن تؤدي برامج التوعية المخصصة إلى زيادة ملحوظة في مستوى الوعي الأمني لدى الإناث، مما يساعد في تقليل نسبة تعرضهن للاختراقات الإلكترونية.

تعزيز المهارات:

– رفع مستوى المهارات والمعرفة التقنية يمكن أن يساعد الأفراد من كلا الجنسين على التعامل مع التهديدات الإلكترونية بفعالية أكبر.

تقليل التفاوتات:

– البرامج التوعوية المتخصصة يمكن أن تسهم في تقليل التفاوت في نسبة التعرض للاختراق بين الذكور والإناث، مما يضمن توافر مستوى عالٍ من الأمان الإلكتروني للجميع.

4. الاستنتاجات

تأثير الجنس على الأمان الإلكتروني:

يلعب الجنس دورًا مهمًا في تحديد مستوى التعرض للاختراقات الإلكترونية. تشير النتائج إلى أن الإناث أكثر عرضة للاختراق، مما يستدعي اهتمامًا خاصًا بتوعيتهن وتزويدهن بالأدوات اللازمة لحماية أنفسهن.

ضرورة التوعية الموجهة:

تشير النتائج إلى أهمية تقديم برامج توعية موجهة تتناسب مع احتياجات كل جنس لضمان وصول الرسالة بفعالية وتحقيق الأهداف المرجوة.

التعاون المجتمعي:

يمكن للتعاون مع المنظمات النسائية والمؤسسات التعليمية أن يسهم بشكل كبير في نشر الوعي الأمني وتحسين مستوى الأمان الإلكتروني بين جميع الفئات.

أهمية التعليم المستمر:

إن التعليم المستمر والتدريب المتخصص ضروريان للحفاظ على مستوى عالٍ من الوعي الأمني. يجب أن تكون البرامج التوعوية مصممة بطريقة تتناسب مع الخلفية التعليمية والاجتماعية للمستهدفين.

يوضح الجدول رقم (05) أن هناك تفاوتًا كبيرًا في نسبة التعرض للاختراق الإلكتروني بين الذكور والإناث، حيث تكون الإناث أكثر عرضة للاختراق. من خلال تقديم برامج توعية مخصصة وتعاون مع المنظمات المجتمعية، يمكن تحسين مستوى الوعي الأمني وتقليل التفاوتات بين الجنسين. التعاون المستمر واستخدام التكنولوجيا كأداة تعليمية يمثلان استراتيجيات فعالة لتحقيق هذا الهدف.

6جدول رقم 06 بين العلاقة بين إتقان استعمال الوسائط التكنولوجية والتعرض للاختراق الالكتروني

الاختراق / استعمال الوسائط التكنولوجية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
جيد	0	00%	15	%21.4	15	%21.4
حسن	0	%00	20	%28.6	20	%28.6
متوسط	13	18.6%	7	%10	20	%28.6
ضعيف	15	%21.4	0	%0	15	%21.4
المجموع	28	%40	42	%60	70	%100

1. تحليل النتائج

الفروق في التعرض للاختراق حسب مستوى الإتقان:

– المستويات "جيد" و"حسن": لم يتعرض أي فرد من الذين يتمتعون بمستوى إتقان "جيد" أو "حسن" للاختراق الإلكتروني، مما يشير إلى أن الأفراد الذين يمتلكون مهارات تقنية جيدة أو حسنة يكونون أقل عرضة للاختراقات.

– المستوى "متوسط": نسبة التعرض للاختراق بين الأفراد ذوي الإتقان المتوسط هي 18.6%، مما يدل على أن هناك بعض الوعي والمهارات، لكن ليس بالشكل الكافي لمنع الاختراقات بشكل كامل.

– المستوى "ضعيف": الأفراد الذين يتمتعون بإتقان ضعيف هم الأكثر عرضة للاختراق بنسبة 21.4%، ولم يتمكن أي فرد من هذه الفئة من تجنب الاختراق، مما يشير إلى ضعف واضح في القدرة على حماية أنفسهم من التهديدات الإلكترونية.

التفاوتات:

– هذه النتائج تعكس أهمية مستوى الإتقان في استخدام الوسائط التكنولوجية في حماية الأفراد من الاختراقات الإلكترونية. فكلما زادت المهارات التقنية، قلت نسبة التعرض للاختراق.

2. التوصيات

برامج توعية وتدريب مخصصة:

– للأفراد ذوي الإتقان الضعيف:

– يجب تطوير برامج تدريبية مكثفة تهدف إلى تحسين مهاراتهم التقنية وتعريفهم بأهم الإجراءات الوقائية لحماية أنفسهم من الاختراقات الإلكترونية. يمكن أن تشمل هذه البرامج ورش عمل ودورات تدريبية متخصصة.

– التركيز على تعليم الأساسيات المهمة مثل كيفية إنشاء كلمات مرور قوية، التعرف على رسائل البريد الإلكتروني الاحتيالية، وأهمية تحديث البرامج بشكل منتظم.

– للأفراد ذوي الإتقان المتوسط:

– يمكن تقديم دورات تدريبية متقدمة لرفع مستواهم من المتوسط إلى الحسن أو الجيد، مع التركيز على التقنيات المتقدمة وأحدث أساليب الحماية الإلكترونية.

– تنظيم جلسات عملية حيث يمكن للمشاركين تطبيق ما تعلموه في بيئة آمنة، مما يعزز من مهاراتهم وثقتهم في التعامل مع التهديدات الإلكترونية.

استراتيجيات التنفيذ:

– التعاون مع المؤسسات التعليمية:

– يمكن التعاون مع المدارس والجامعات لتقديم برامج تعليمية متخصصة في الأمان الإلكتروني ضمن المناهج الدراسية. يمكن أن تشمل هذه البرامج دروسًا نظرية وعملية تعزز من مهارات الطلاب التقنية.

– تطوير منصات تعليمية عبر الإنترنت تقدم مواد تعليمية تفاعلية ومحدثة باستمرار حول الأمان الإلكتروني.

– استخدام وسائل الإعلام والتواصل الاجتماعي:

– استغلال وسائل الإعلام والتواصل الاجتماعي لنشر محتوى توعوي يستهدف جميع مستويات الإتقان، مع التركيز على النصائح العملية والتحديثات المستمرة حول أحدث التهديدات وأساليب الحماية.

– إنشاء حملات توعوية تتضمن فيديوهات تعليمية، مقالات، واختبارات تفاعلية يمكن أن تساعد في تقييم وتحسين مستوى الإتقان لدى الأفراد.

3. النتائج

تحسين الوعي الأمني:

من المتوقع أن تؤدي برامج التوعية والتدريب المخصصة إلى زيادة ملحوظة في مستوى الوعي الأمني بين الأفراد ذوي الإتقان الضعيف والمتوسط، مما يساعد في تقليل نسبة تعرضهم للاختراقات الإلكترونية.

تعزيز المهارات التقنية:

يمكن لرفع مستوى المهارات والمعرفة التقنية أن يساعد الأفراد على التعامل مع التهديدات الإلكترونية بفعالية أكبر، مما يقلل من احتمالية التعرض للاختراقات الأمنية.

تقليل الفجوة التعليمية:

يمكن لبرامج التوعوية المتخصصة أن تسهم في تقليل الفجوة في مستوى المهارات التقنية بين الأفراد، مما يضمن توافر مستوى عالٍ من الأمان الإلكتروني للجميع.

4. الاستنتاجات

تأثير مستوى الإتقان على الأمان الإلكتروني:

يلعب مستوى الإتقان في استعمال الوسائط التكنولوجية دورًا حاسمًا في تحديد مدى التعرض للاختراقات الإلكترونية. الأفراد ذوي الإتقان الجيد أو الحسن أقل عرضة للاختراقات، مما يعكس أهمية التعليم والتدريب المستمر في هذا المجال.

ضرورة التوعية الموجهة:

تشير النتائج إلى أهمية تقديم برامج توعية موجهة تتناسب مع مستوى المهارات التقنية للأفراد لضمان وصول الرسالة بفعالية وتحقيق الأهداف المرجوة.

التعاون المجتمعي:

يمكن للتعاون مع المؤسسات التعليمية والمجتمعية أن يسهم بشكل كبير في نشر الوعي الأمني وتحسين مستوى الأمان الإلكتروني بين جميع الفئات.

أهمية التعليم المستمر:

إن التعليم المستمر والتدريب المتخصص ضروريان للحفاظ على مستوى عالٍ من الوعي الأمني. يجب أن تكون البرامج التوعوية مصممة بطريقة تتناسب مع الخلفية التعليمية والتقنية للمستهدفين.

يوضح الجدول رقم (06) أن هناك تفاوتًا كبيرًا في نسبة التعرض للاختراق الإلكتروني بناءً على مستوى الإتقان في استعمال الوسائط التكنولوجية. من خلال تقديم برامج توعية وتدريب مخصصة وتعاون مع المؤسسات المجتمعية، يمكن تحسين مستوى الوعي الأمني وتقليل الفجوة بين مختلف مستويات المهارات التقنية. التعليم المستمر واستخدام التكنولوجيا كأداة تعليمية يمثلان استراتيجيات فعالة لتحقيق هذا الهدف.

7جدول رقم 07 يبين العلاقة بين التصريح بالهوية الكترونيا والتعرض للاختراق الالكتروني

الاختراق / التصريح بالهوية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
نعم	21	%30	20	%28.6	41	%58.6
لا	7	%10	22	%31.4	29	%41.4
المجموع	28	%40	42	%60	70	%100

1. تحليل النتائج

الفروق في التعرض للاختراق حسب التصريح بالهوية:

- التصريح بالهوية إلكترونيًا:

- نسبة التعرض للاختراق بين الأفراد الذين يصرحون بهويتهم إلكترونيًا هي 30%. وهذا يشير إلى أن التصريح بالهوية قد يزيد من احتمالية التعرض للاختراقات الإلكترونية.

- نسبة الأفراد الذين لم يتعرضوا للاختراق بينهم هي 28.6%.

- عدم التصريح بالهوية إلكترونيًا:

- نسبة التعرض للاختراق بين الأفراد الذين لا يصرحون بهويتهم إلكترونيًا هي 10% فقط، مما يشير إلى أن عدم التصريح بالهوية يمكن أن يقلل من احتمالية التعرض للاختراقات.

- نسبة الأفراد الذين لم يتعرضوا للاختراق بينهم هي 31.4%.

التفاوتات:

- تشير البيانات إلى أن التصريح بالهوية إلكترونيًا يزيد من احتمالية التعرض للاختراقات الإلكترونية مقارنة بعدم التصريح. يمكن أن يكون السبب وراء ذلك هو زيادة كمية المعلومات الشخصية المتاحة عبر الإنترنت، مما يجعل الأفراد أهدافًا أسهل للقراصنة.

2. التوصيات

برامج توعية وتدريب مخصصة:

- للأفراد الذين يصرحون بهويتهم إلكترونيًا:

– يجب تعليمهم أهمية حماية معلوماتهم الشخصية وكيفية استخدام وسائل الأمان المتاحة مثل كلمات المرور القوية، التحقق بخطوتين، والحذر من الرسائل المشبوهة.

– توعية الأفراد بمخاطر التصريح بالهوية إلكترونيًا وكيفية تقليل هذه المخاطر من خلال تقليل كمية المعلومات التي يشاركونها عبر الإنترنت.

– للأفراد الذين لا يصرحون بهويتهم إلكترونيًا:

– توجيههم للحفاظ على مستوى الأمان الحالي وتعليمهم كيفية الحفاظ على معلوماتهم الشخصية آمنة دون الحاجة إلى التصريح بالهوية إلكترونيًا.

استراتيجيات التنفيذ:

– التعاون مع المؤسسات التعليمية:

– تنظيم دورات تدريبية وورش عمل في المدارس والجامعات لزيادة وعي الطلاب حول مخاطر التصريح بالهوية إلكترونيًا وكيفية حماية معلوماتهم الشخصية.

– تقديم ندوات عبر الإنترنت تتضمن نصائح عملية ومحدثة حول الأمان الإلكتروني.

– استخدام وسائل التواصل الاجتماعي:

– استغلال منصات التواصل الاجتماعي لنشر محتوى توعوي حول الأمان الإلكتروني والتركيز على مخاطر التصريح بالهوية إلكترونيًا.

– إنشاء حملات توعوية تستهدف الجمهور العريض وتستخدم فيديوهات تعليمية ومقالات ونصائح تفاعلية.

3. النتائج

تحسين الوعي الأمني:

– من المتوقع أن تؤدي برامج التوعية إلى زيادة ملحوظة في مستوى الوعي الأمني بين الأفراد الذين يصرحون بهويتهم إلكترونيًا، مما يساعد في تقليل نسبة تعرضهم للاختراقات.

تعزيز المهارات:

– رفع مستوى المهارات والمعرفة التقنية يمكن أن يساعد الأفراد على التعامل مع التهديدات الإلكترونية بفعالية أكبر وتقليل احتمالية تعرضهم للاختراقات.

تقليل التفاوتات:

– البرامج التوعوية المتخصصة يمكن أن تسهم في تقليل الفجوة في مستوى الأمان بين الأفراد الذين يصرحون بهويتهم إلكترونيًا والأفراد الذين لا يصرحون بها.

4. الاستنتاجات

تأثير التصريح بالهوية على الأمان الإلكتروني:

– التصريح بالهوية إلكترونيًا يزيد من احتمالية التعرض للاختراقات الإلكترونية، مما يستدعي اهتمامًا خاصًا بتوعية الأفراد حول مخاطر التصريح بالهوية وكيفية حماية معلوماتهم الشخصية.

ضرورة التوعية الموجهة:

– النتائج تشير إلى أهمية تقديم برامج توعية موجهة تتناسب مع سلوك الأفراد في التصريح بالهوية إلكترونيًا لضمان وصول الرسالة بفعالية وتحقيق الأهداف المرجوة.

التعاون المجتمعي:

– التعاون مع المؤسسات التعليمية والمجتمعية يمكن أن يسهم بشكل كبير في نشر الوعي الأمني وتحسين مستوى الأمان الإلكتروني بين جميع الفئات.

أهمية التعليم المستمر:

– التعليم المستمر والتدريب المتخصص ضروريان للحفاظ على مستوى عالٍ من الوعي الأمني. يجب أن تكون البرامج التوعوية مصممة بطريقة تتناسب مع الخلفية التعليمية والسلوكية للمستهدفين.

يوضح الجدول رقم (07) أن هناك تفاوتًا كبيرًا في نسبة التعرض للاختراق الإلكتروني بناءً على التصريح بالهوية إلكترونيًا. من خلال تقديم برامج توعية وتدريب مخصصة وتعاون مع المؤسسات المجتمعية، يمكن تحسين مستوى الوعي الأمني وتقليل الفجوة بين الأفراد الذين يصرحون بهويتهم إلكترونيًا والأفراد الذين لا يصرحون بها. التعليم المستمر واستخدام التكنولوجيا كأداة تعليمية يمثلان استراتيجيات فعالة لتحقيق هذا الهدف.

8جدول رقم 08 يبين العلاقة بين التعرض للاختراق الالكتروني ومدى خوف المبحوثين للاختراق

الخوف من الاختراق / الاختراق	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
نعم	21	%30	7	%10	28	40%
لا	21	%30	21	30%	42	60%
المجموع	42	%60	28	%40	70	%100

يتناول هذا الجدول العلاقة بين تعرض الأفراد للاختراق الإلكتروني ومدى خوفهم من الاختراق، وهو جزء من دراسة أوسع حول الوعي الأمني وعلاقته بالجريمة المعلوماتية في المجتمع الجزائري. يوضح الجدول عدد ونسبة المبحوثين الذين تعرضوا للاختراق الإلكتروني ومدى خوفهم من التعرض لهذا النوع من الجرائم.

1. تحليل البيانات

أولاً: التعرض للاختراق الإلكتروني:

– 60% من المبحوثين تعرضوا للاختراق الإلكتروني، مما يشير إلى انتشار واسع لهذه الظاهرة في المجتمع.

– 40% من المبحوثين لم يتعرضوا للاختراق الإلكتروني، وهو نسبة أقل بكثير مما يعكس خطورة انتشار الجرائم المعلوماتية.

ثانياً: الخوف من الاختراق الإلكتروني:

– 40% من المبحوثين يخافون من التعرض للاختراق الإلكتروني، وهو نسبة مهمة تشير إلى وجود وعي بخطورة هذه الجرائم.

– 60% من المبحوثين لا يخافون من الاختراق الإلكتروني، مما قد يشير إلى قلة الوعي أو الثقة المفرطة في الحماية الشخصية ضد هذه الجرائم.

ثالثاً: العلاقة بين التعرض والخوف:

– خائفون وتعرضوا للاختراق: 21 مبحوث (30% من الإجمالي) تعرضوا للاختراق ويشعرون بالخوف، مما يدل على أن التجربة الفعلية للاختراق تساهم في زيادة الخوف.

– خائفون ولم يتعرضوا للاختراق: 7 مبحوثين (10% من الإجمالي) يخافون من الاختراق دون أن يكونوا قد تعرضوا له، وهذا قد يشير إلى وعيهم بخطورة الجرائم المعلوماتية.

– غير خائفين وتعرضوا للاختراق: 21 مبحوث (30% من الإجمالي) تعرضوا للاختراق لكنهم لا يخافون، مما قد يدل على إما استهانة بخطورة الجرائم أو اعتقادهم بأنهم تعلموا كيفية تجنبها مستقبلاً.

– غير خائفين ولم يتعرضوا للاختراق: 21 مبحوث (30% من الإجمالي) لم يتعرضوا للاختراق ولا يخافون منه، مما يعكس ثقة مفرطة أو قلة وعي بخطورة الجرائم المعلوماتية.

2. القرار والتوصيات

القرار: بناءً على هذه البيانات، يتضح أن هناك حاجة ملحة لتعزيز الوعي الأمني لدى المجتمع الجزائري لمواجهة الجرائم المعلوماتية بشكل أكثر فعالية.

التوصيات:

1. حملات توعية مكثفة: تنفيذ حملات توعية تستهدف جميع الفئات العمرية والتعليمية لرفع مستوى الوعي بخطورة الجرائم المعلوماتية وكيفية الحماية منها.

2. برامج تدريبية: تطوير برامج تدريبية متخصصة حول الأمان الإلكتروني لتعليم الأفراد كيفية حماية أنفسهم من الاختراق.

3. تعزيز القوانين: تشديد القوانين والعقوبات المتعلقة بالجرائم المعلوماتية لردع المجرمين وحماية الأفراد.

4. التعاون مع المؤسسات التعليمية: إدراج مواضيع الأمن الإلكتروني في المناهج التعليمية لزيادة الوعي بين الشباب.

5. الدعم التقني: توفير دعم تقني ومراكز مساعدة للأفراد الذين تعرضوا للاختراق لمساعدتهم على استعادة أمن معلوماتهم.

3. النتائج

– نسبة عالية من التعرض: يشير تعرض 60% من المبحوثين للاختراق الإلكتروني إلى انتشار واسع لهذه الظاهرة في المجتمع الجزائري.

– وعي متفاوت: هناك تفاوت في مستوى الوعي بالخطر بين الأفراد، حيث أن 40% فقط يخافون من التعرض للاختراق، مما يستدعي جهودًا أكبر في التوعية.

– أثر التجربة: التجربة الفعلية للاختراق تؤثر بشكل كبير على الخوف من التعرض له، حيث أن الأفراد الذين تعرضوا للاختراق يميلون إلى الخوف بشكل أكبر.

4. الاستنتاجات

– ضرورة الوعي الأمني: تعزيز الوعي الأمني هو أمر ضروري لمكافحة الجرائم المعلوماتية بشكل فعال.

– الفجوة في الوعي: هناك فجوة في الوعي بخطورة الجرائم المعلوماتية بين المبحوثين، مما يتطلب تدخلات توعوية وتعليمية مركزة.

– أثر التجربة الشخصية: التجارب الشخصية مع الاختراق تؤثر بشكل كبير على مستوى الخوف والوعي بخطورة الجرائم، مما يعني أن نشر تجارب الآخرين قد يكون أداة فعالة في حملات التوعية.

في الختام، يعد هذا الجدول دليلاً واضحاً على أهمية الوعي الأمني في حماية الأفراد من الجرائم المعلوماتية وضرورة اتخاذ خطوات فعالة لزيادة هذا الوعي في المجتمع الجزائري.

9جدول رقم 09 يبين العلاقة بين التعرض للاختراق الالكتروني وسبب الاختراق من منظور المبحوثين

سبب من الاختراق / الاختراق	الضحية		الجاني		المجموع	
	ك	%	ك	%	ك	%
نعم	0	20%	28	40%	28	40%
لا	28	40%	14	20%	42	60%
المجموع	28	%40	42	60%	70	%100

يتناول الجدول رقم 09 العلاقة بين تعرض الأفراد للاختراق الإلكتروني وأسباب هذا الاختراق من منظور المبحوثين، سواء كانوا يعتقدون أن السبب هو الضحية (المستخدم) أو الجاني (المخترق).

1. تحليل البيانات

أولاً: التعرض للاختراق الإلكتروني:

- 40% من المبحوثين تعرضوا للاختراق الإلكتروني، مما يعكس انتشار هذه الظاهرة في المجتمع.

- 60% من المبحوثين لم يتعرضوا للاختراق الإلكتروني، مما يعني أن الأغلبية لم تختبر هذه التجربة مباشرة.

ثانياً: سبب الاختراق من منظور المبحوثين:

– الضحية (المستخدم): 40% من المبحوثين يعتقدون أن السبب في الاختراق يعود إلى الضحية نفسها.

– الجاني (المخترق): 60% من المبحوثين يرون أن الجاني هو السبب الرئيسي في حدوث الاختراق.

ثالثاً: العلاقة بين التعرض للاختراق وسبب الاختراق:

– نعم، الضحية: لا يوجد مبحوث تعرض للاختراق يعتقد أن السبب هو الضحية، مما يشير إلى أن الذين تعرضوا للاختراق يميلون إلى لوم المخترقين وليس أنفسهم.

– نعم، الجاني: 28 مبحوث (40% من الإجمالي) تعرضوا للاختراق ويعتقدون أن الجاني هو السبب، مما يعكس وعيهم بأساليب الاختراق وعدم لوم أنفسهم.

– لا، الضحية: 28 مبحوث (40% من الإجمالي) لم يتعرضوا للاختراق ولكن يعتقدون أن السبب يعود إلى الضحية، مما قد يشير إلى وعيهم بمخاطر السلوك غير الآمن على الإنترنت.

– لا، الجاني: 14 مبحوث (20% من الإجمالي) لم يتعرضوا للاختراق ويعتقدون أن الجاني هو السبب، مما يدل على أنهم يرون في المخترقين التهديد الرئيسي.

2. القرار والتوصيات

القرار:

بناءً على هذه البيانات، يتضح أن هناك تفاوت في وجهات النظر حول أسباب الاختراق الإلكتروني بين الذين تعرضوا له والذين لم يتعرضوا، مما يتطلب تدخلات تعليمية وتوعوية لتعزيز الفهم الصحيح لهذه الظاهرة.

التوصيات:

1. توعية حول سلوكيات الأمان: توعية المستخدمين حول أهمية السلوكيات الآمنة على الإنترنت وكيفية تجنب الأخطاء التي قد تؤدي إلى الاختراق.

2. دورات تدريبية: تقديم دورات تدريبية حول كيفية التعرف على أساليب الاختراق والتعامل معها.

3. حملات توعية: تنظيم حملات توعية لزيادة الفهم حول دور كل من المستخدم والمخترق في حدوث الجرائم المعلوماتية.

4. دعم فني: توفير دعم فني مستمر لمساعدة المستخدمين في حماية معلوماتهم الشخصية وتقديم نصائح وقائية.

5. تعزيز القوانين: تشديد العقوبات على الجرائم المعلوماتية لتقليل الدوافع لدى الجناة وزيادة الردع.

3. النتائج

– تفاوت في الفهم: هناك تفاوت في فهم أسباب الاختراق بين المبحوثين، مما يعكس حاجة ماسة للتوعية.

– أهمية الوعي الأمني: الوعي الأمني يلعب دوراً كبيراً في حماية المستخدمين، حيث أن الذين لم يتعرضوا للاختراق يظهرون وعياً أكبر بمخاطر السلوك غير الآمن.

– دور الجاني: معظم المبحوثين يرون أن الجاني هو السبب الرئيسي في الاختراق، مما يشير إلى الاعتراف بخطورة الهجمات الإلكترونية.

4. الاستنتاجات

– زيادة الوعي: من الضروري زيادة الوعي بين المستخدمين حول دورهم في حماية معلوماتهم الشخصية وكيفية تجنب السلوكيات التي تسهل على المخترقين.

– توزيع المسؤولية: يجب توضيح أن حماية المعلومات تتطلب جهوداً مشتركة بين الأفراد والمؤسسات لتقليل مخاطر الاختراق.

– التعليم والتدريب: تعزيز التعليم والتدريب في مجال الأمن الإلكتروني سيساهم بشكل كبير في تقليل حوادث الاختراق وزيادة الأمان.

في الختام، يظهر هذا الجدول الحاجة الملحة إلى تعزيز الوعي الأمني بين أفراد المجتمع الجزائري وفهم أعمق لدور كل من المستخدم والمخترق في حدوث الجرائم المعلوماتية.

الفرضية الثانية

10جدول رقم (10) يبين العلاقة بين الفئة العمرية للمبحوثين التعرض للاختراق الإلكتروني

التعرض للاختراق / الفئة العمرية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
من 18 21	6	%8.6	15	%21.4	21	30%
اكثر من 21سنة	22	%31.4	27	38.4%	49	70%
المجموع	28	40%	42	60%	70	%100

يتناول الجدول رقم 10 العلاقة بين الفئة العمرية للمبحوثين ومدى تعرضهم للاختراق الإلكتروني. يوضح الجدول توزيع المبحوثين حسب الفئة العمرية وحالة تعرضهم للاختراق، مما يساعد في فهم مدى تأثير العمر على احتمال التعرض لهذه الجرائم.

1. تحليل البيانات

أولاً: الفئة العمرية من 18 إلى 21 سنة:

– تعرضوا للاختراق: 8.6% من هذه الفئة تعرضوا للاختراق الإلكتروني. هذه النسبة منخفضة نسبياً.

– لم يتعرضوا للاختراق: 21.4% من هذه الفئة لم يتعرضوا للاختراق. هذه النسبة تشير إلى أن الأغلبية في هذه الفئة العمرية لم تختبر هذه التجربة.

ثانياً: الفئة العمرية أكثر من 21 سنة:

– تعرضوا للاختراق: 31.4% من هذه الفئة تعرضوا للاختراق الإلكتروني. هذه النسبة أعلى بكثير مقارنة بالفئة الأصغر سناً، مما يشير إلى أن الأفراد الأكبر سناً أكثر عرضة للاختراق.

– لم يتعرضوا للاختراق: 38.4% من هذه الفئة لم يتعرضوا للاختراق، وهي نسبة كبيرة أيضاً ولكن أقل من الذين تعرضوا للاختراق.

ثالثاً: العلاقة بين الفئة العمرية والتعرض للاختراق:

– من 18 إلى 21 سنة: 30% من المبحوثين في هذه الفئة العمرية. تشير البيانات إلى أن هذه الفئة لديها وعي أقل أو قد تكون أقل استهدافاً.

– أكثر من 21 سنة: 70% من المبحوثين في هذه الفئة العمرية. تشير النسبة العالية للتعرض للاختراق في هذه الفئة إلى أن الأفراد الأكبر سناً قد يكون لديهم تواجد أكبر على الإنترنت أو يقومون بأنشطة أكثر عرضة للاختراق.

2. القرار والتوصيات

القرار:

يتضح من البيانات أن الأفراد في الفئة العمرية أكثر من 21 سنة هم الأكثر عرضة للاختراق الإلكتروني مقارنة بالفئة العمرية من 18 إلى 21 سنة. يتطلب ذلك تدخلات مخصصة لكل فئة عمرية لرفع الوعي وتعزيز الأمان الإلكتروني.

التوصيات:

1. حملات توعية موجهة: تطوير حملات توعية مخصصة لكل فئة عمرية، مع التركيز على الفئة الأكبر سناً نظراً لارتفاع نسبة تعرضهم للاختراق.

2. تعليم الأمان الإلكتروني: إدراج برامج تعليمية حول الأمان الإلكتروني في المناهج الدراسية للطلاب من 18 إلى 21 سنة لتعزيز الوعي في سن مبكرة.

3. برامج تدريب متقدمة: تقديم برامج تدريب متقدمة للأفراد فوق 21 سنة لتعليمهم كيفية حماية أنفسهم من الهجمات الإلكترونية.

4. تطوير أدوات حماية: توفير أدوات حماية سهلة الاستخدام وفعالة تتناسب مع احتياجات كل فئة عمرية.

5. تعاون مع المؤسسات: العمل مع المؤسسات المختلفة لتوفير ورش عمل وحلقات نقاش حول الأمان الإلكتروني للفئات العمرية المختلفة.

3. النتائج

– الفئة الأكبر سناً أكثر عرضة: الأفراد في الفئة العمرية أكثر من 21 سنة هم الأكثر تعرضاً للاختراق الإلكتروني، مما يتطلب اهتماماً خاصاً.

– حاجة للتوعية المبكرة: الفئة العمرية من 18 إلى 21 سنة تحتاج إلى تعزيز الوعي بالأمان الإلكتروني في مرحلة مبكرة لتجنب المخاطر المستقبلية.

– توزيع مستهدف للموارد: يجب تخصيص الموارد بشكل مستهدف لكل فئة عمرية لضمان تحقيق أقصى قدر من الحماية والأمان.

4. الاستنتاجات

– أهمية العمر في التعرض للاختراق: العمر يلعب دوراً مهماً في احتمالية التعرض للاختراق الإلكتروني، مع زيادة الاحتمالية بين الأفراد الأكبر سناً.

– تخصيص الجهود التوعوية: من الضروري تخصيص الجهود التوعوية والتدريبية بما يتناسب مع الفئات العمرية المختلفة لتحقيق أقصى فعالية في مكافحة الجرائم المعلوماتية.

– التدخل المبكر: التدخل المبكر من خلال التعليم والتوعية يمكن أن يقلل من مخاطر التعرض للاختراق في المستقبل.

في الختام، يعكس هذا الجدول أهمية التركيز على الفئات العمرية المختلفة عند تصميم استراتيجيات الحماية والتوعية ضد الجرائم المعلوماتية.

11جدول رقم (11) يبين العلاقة بين المستوى الجامعي للمبحوثين التعرض للاختراق الإلكتروني

التعرض للاختراق / مستوي الجامعي	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
ليسانس	14	20%	22	%21.4	36	%51.1
ماستر	14	%20	20	38.4%	34	48.4%
المجموع	28	40%	42	60%	70	%100

يتناول الجدول رقم 11 العلاقة بين المستوى الجامعي للمبحوثين ومدى تعرضهم للاختراق الإلكتروني. يوضح الجدول توزيع المبحوثين حسب المستوى الجامعي وحالة تعرضهم للاختراق، مما يساعد في فهم تأثير التعليم الجامعي على احتمال التعرض لهذه الجرائم.

1. تحليل البيانات

أولاً: مستوى التعليم (ليسانس):

- تعرضوا للاختراق: 20% من هذه الفئة تعرضوا للاختراق الإلكتروني.
- لم يتعرضوا للاختراق: 31.4% من هذه الفئة لم يتعرضوا للاختراق.
- المجموع: 51.4% من المبحوثين هم من حملة شهادة الليسانس.

ثانياً: مستوى التعليم (ماستر):

- تعرضوا للاختراق: 20% من هذه الفئة تعرضوا للاختراق الإلكتروني.

- لم يتعرضوا للاختراق: 28.6% من هذه الفئة لم يتعرضوا للاختراق.

- المجموع: 48.6% من المبحوثين هم من حملة شهادة الماستر.

ثالثاً: العلاقة بين المستوى الجامعي والتعرض للاختراق:

- ليسانس: 51.4% من المبحوثين يحملون شهادة الليسانس. نسبة التعرض للاختراق في هذه الفئة هي 20%.

- ماستر: 48.6% من المبحوثين يحملون شهادة الماستر. نسبة التعرض للاختراق في هذه الفئة هي 20%.

2. القرار والتوصيات

القرار: بناءً على البيانات، يتضح أن مستوى التعليم الجامعي لا يؤثر بشكل كبير على احتمالية التعرض للاختراق الإلكتروني، حيث أن نسبة التعرض للاختراق هي نفسها في كلا الفئتين (ليسانس وماستر).

التوصيات:

1. تعزيز التوعية في جميع المستويات الجامعية: توفير برامج توعية حول الأمان الإلكتروني لجميع الطلاب بغض النظر عن مستواهم التعليمي.

2. دورات متخصصة: تقديم دورات تدريبية متقدمة لحملة شهادتي الليسانس والماستر لتعليمهم كيفية حماية أنفسهم من الهجمات الإلكترونية.

3. تكثيف الحملات التوعوية: تنظيم حملات توعية داخل الجامعات لتسليط الضوء على أهمية الأمان الإلكتروني.

4. تعاون بين المؤسسات التعليمية: التعاون بين الجامعات والمؤسسات المختصة في مجال الأمان الإلكتروني لتوفير موارد تعليمية ودعم فني للطلاب.

5. إدراج الأمان الإلكتروني في المناهج: دمج مفاهيم الأمان الإلكتروني ضمن المناهج الدراسية للطلاب في جميع المستويات الجامعية.

3. النتائج

– نسبة متساوية للتعرض: الفئتان (ليسانس وماستر) تتعرضان للاختراق بنفس النسبة (20%)، مما يشير إلى أن مستوى التعليم الجامعي لا يؤثر بشكل كبير على احتمالية التعرض للاختراق.

– حاجة للتوعية المستمرة: الحاجة لتوفير التوعية والتدريب المستمر في مجال الأمان الإلكتروني بغض النظر عن المستوى التعليمي.

– التعاون المؤسسي: ضرورة التعاون بين المؤسسات التعليمية والمتخصصة لتعزيز الأمان الإلكتروني بين الطلاب.

4. الاستنتاجات

– أهمية التوعية: التعليم الجامعي لوحده لا يضمن الحماية من الاختراق الإلكتروني، مما يؤكد الحاجة إلى حملات توعية وتدريب مستمر.

– التدخل الشامل: ضرورة التدخل الشامل في جميع مستويات التعليم الجامعي لضمان تحقيق أعلى مستويات الأمان الإلكتروني.

– دور المؤسسات التعليمية: يجب أن تلعب المؤسسات التعليمية دوراً أكبر في تعزيز الوعي بالأمان الإلكتروني وتقديم الدعم المستمر للطلاب.

في الختام، يظهر هذا الجدول أهمية التركيز على تعزيز الأمان الإلكتروني بين الطلاب الجامعيين بغض النظر عن مستواهم التعليمي، وذلك من خلال التوعية والتدريب المستمر والتعاون بين المؤسسات المختلفة.

12جدول رقم (12) يبين العلاقة بين المستوى الجامعي للمبحوثين والمداومة على التجوال في الحقل المعلوماتي

المدوامة على تجول الالكتروني / مستوي الجامعي	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
ليسانس	29	41.4%	7	%10	36	% 51.4
ماستر	27	%38.6	4	10%	34	48.6%
المجموع	56	80%	14	20%	70	%100

يتناول الجدول رقم 12 العلاقة بين المستوى الجامعي للمبحوثين ومدى مداومتهم على التجوال في الحقل المعلوماتي. يوضح الجدول توزيع المبحوثين حسب المستوى الجامعي وحالة مداومتهم على التجوال الإلكتروني، مما يساعد في فهم تأثير المستوى التعليمي على النشاط في الحقل المعلوماتي.

1. تحليل البيانات

أولاً: مستوى التعليم (ليسانس):

– مداومون على التجوال: 41.4% من حملة الليسانس مداومون على التجوال في الحقل المعلوماتي.

– غير مداومين على التجوال: 10% من حملة الليسانس غير مداومين على التجوال في الحقل المعلوماتي.

– المجموع: 51.4% من المبحوثين هم من حملة الليسانس.

ثانياً: مستوى التعليم (ماستر):

– مداومون على التجوال: 38.6% من حملة الماستر مداومون على التجوال في الحقل المعلوماتي.

– غير مداومين على التجوال: 10% من حملة الماستر غير مداومين على التجوال في الحقل المعلوماتي.

– المجموع: 48.6% من المبحوثين هم من حملة الماستر.

ثالثاً: العلاقة بين المستوى الجامعي والمداومة على التجوال الإلكتروني:

– نعم (مداومون): 80% من المبحوثين مداومون على التجوال في الحقل المعلوماتي.

– لا (غير مداومين): 20% من المبحوثين غير مداومين على التجوال في الحقل المعلوماتي.

2. القرار والتوصيات

القرار:

يتضح من البيانات أن أغلبية المبحوثين، بغض النظر عن مستواهم التعليمي، مداومون على التجوال في الحقل المعلوماتي بنسبة 80%. الفارق بين حملة الليسانس وحملة الماستر ليس كبيرًا فيما يخص المداومة على التجوال الإلكتروني.

التوصيات:

1. تعزيز التوعية الأمنية: نظراً لأن معظم المبحوثين مداومون على التجوال في الحقل المعلوماتي، ينبغي تعزيز التوعية بالأمن الإلكتروني لجميع الطلاب.

2. برامج تعليمية وتدريبية: توفير برامج تعليمية وتدريبية تشمل جميع مستويات التعليم الجامعي لتعزيز ممارسات الأمان الإلكتروني.

3. تطوير أدوات الحماية: تطوير أدوات حماية متقدمة وسهلة الاستخدام تساعد الطلاب في حماية معلوماتهم أثناء التجوال في الحقل المعلوماتي.

4. حملات توعية مخصصة: تنظيم حملات توعية مخصصة لكل مستوى تعليمي، مع التركيز على أهمية الأمان الإلكتروني وتجنب المخاطر المحتملة.

5. تشجيع الممارسات الآمنة: تشجيع الممارسات الآمنة وتبادل الخبرات بين الطلاب حول كيفية الحفاظ على الأمان أثناء التجوال الإلكتروني.

3. النتائج

– معدل المداومة المرتفع: نسبة كبيرة من المبحوثين (80%) مداومون على التجوال في الحقل المعلوماتي، مما يعكس انتشار هذا النشاط بينهم.

– توزيع متساوٍ نسبياً: لا يوجد فارق كبير بين حملة الليسانس والماستر فيما يتعلق بمعدل المداومة على التجوال الإلكتروني، مما يشير إلى أن مستوى التعليم لا يؤثر بشكل كبير على هذا النشاط.

– حاجة للأمان الإلكتروني: ارتفاع معدل المداومة على التجوال الإلكتروني يتطلب تعزيز الوعي والممارسات الآمنة بين الطلاب.

4. الاستنتاجات

– ضرورة التوعية الأمنية: يجب التركيز على التوعية بالأمان الإلكتروني لجميع الطلاب بغض النظر عن مستواهم التعليمي، نظراً لارتفاع نسبة المداومين على التجوال الإلكتروني.

– التعليم المستمر: من الضروري توفير برامج تعليمية مستمرة تركز على الأمان الإلكتروني وتواكب التطورات في هذا المجال.

– دعم الممارسات الآمنة: دعم الممارسات الآمنة والتشجيع على تبنيها بين الطلاب يمكن أن يساهم في تقليل المخاطر المرتبطة بالتجوال الإلكتروني.

في الختام، يعكس هذا الجدول أهمية تعزيز الأمان الإلكتروني بين الطلاب الجامعيين نظراً لارتفاع معدل مداومتهم على التجوال في الحقل المعلوماتي، مما يتطلب تدخلات تعليمية وتوعوية مستمرة.

13جدول رقم (13) يبين العلاقة بين الفئة العمرية للمبحوثين والمداومة على التجوال في الحقل المعلوماتي

المداومةا على التجول الالكتروانيلفئة العمرية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
من 18 21	14	20%	7	%10	21	30%
اكثر من 21سنة	42	%60	7	10%	49	70%
المجموع	56	80%	14	%20	70	%100

يتناول الجدول رقم 13 العلاقة بين الفئة العمرية للمبحوثين ومدى مداومتهم على التجوال في الحقل المعلوماتي. يوضح الجدول توزيع المبحوثين حسب الفئة العمرية وحالة مداومتهم على التجوال الإلكتروني، مما يساعد في فهم تأثير العمر على النشاط في الحقل المعلوماتي.

1. تحليل البيانات

أولاً: الفئة العمرية من 18 إلى 21 سنة:

– مداومون على التجوال: 20% من المبحوثين في هذه الفئة العمرية مداومون على التجوال في الحقل المعلوماتي.

– غير مداومين على التجوال: 10% من المبحوثين في هذه الفئة العمرية غير مداومين على التجوال في الحقل المعلوماتي.

– المجموع: 30% من المبحوثين هم من الفئة العمرية من 18 إلى 21 سنة.

ثانياً: الفئة العمرية أكثر من 21 سنة:

– مداومون على التجوال: 60% من المبحوثين في هذه الفئة العمرية مداومون على التجوال في الحقل المعلوماتي.

– غير مداومين على التجوال: 10% من المبحوثين في هذه الفئة العمرية غير مداومين على التجوال في الحقل المعلوماتي.

– المجموع: 70% من المبحوثين هم من الفئة العمرية أكثر من 21 سنة.

ثالثاً: العلاقة بين الفئة العمرية والمداومة على التجوال الإلكتروني:

– نعم (مداومون): 80% من المبحوثين مداومون على التجوال في الحقل المعلوماتي.

– لا (غير مداومين): 20% من المبحوثين غير مداومين على التجوال في الحقل المعلوماتي.

2. القرار والتوصيات

القرار:

بناءً على البيانات، يتضح أن الأفراد في الفئة العمرية أكثر من 21 سنة يميلون بشكل أكبر إلى المداومة على التجوال في الحقل المعلوماتي مقارنة بالفئة العمرية من 18 إلى 21 سنة.

التوصيات:

1. تعزيز التوعية الأمنية للفئات المختلفة: نظرًا لأن نسبة كبيرة من الأفراد من جميع الفئات العمرية مداومون على التجوال، يجب تعزيز التوعية بالأمان الإلكتروني للجميع.

2. برامج تدريبية موجهة: تطوير برامج تدريبية موجهة لكل فئة عمرية، مع التركيز على الفئة العمرية أكثر من 21 سنة نظرًا لنشاطهم المرتفع في الحقل المعلوماتي.

3. توفير الموارد والدعم: توفير موارد ودعم مستمر للأفراد في جميع الفئات العمرية لتعزيز ممارسات الأمان الإلكتروني.

4. تشجيع الممارسات الآمنة: تشجيع الأفراد على تبني ممارسات آمنة أثناء التجوال في الحقل المعلوماتي من خلال ورش عمل وحملات توعية.

5. التعاون مع المؤسسات التعليمية: التعاون مع المؤسسات التعليمية لتضمين الأمان الإلكتروني ضمن المناهج الدراسية وبرامج التوعية.

3. النتائج

– نشاط مرتفع بين الأكبر سنًا: الأفراد في الفئة العمرية أكثر من 21 سنة هم الأكثر مداومة على التجوال في الحقل المعلوماتي بنسبة 60%.

– حاجة للتوعية المستمرة: الحاجة لتوعية مستمرة لجميع الفئات العمرية، حيث أن نسبة المداومة على التجوال مرتفعة بشكل عام.

– دور المؤسسات التعليمية: المؤسسات التعليمية يمكن أن تلعب دورًا مهمًا في تعزيز الأمان الإلكتروني بين الأفراد من جميع الفئات العمرية.

4. الاستنتاجات

– تأثير العمر على النشاط المعلوماتي: العمر له تأثير واضح على النشاط في الحقل المعلوماتي، مع زيادة المداومة على التجوال بين الأفراد الأكبر سنًا.

– أهمية التوعية الشاملة: من الضروري توفير توعية شاملة ومستمرة لجميع الفئات العمرية لضمان الحماية الفعالة أثناء التجوال الإلكتروني.

– التعاون المؤسسي: التعاون بين المؤسسات التعليمية والمؤسسات المتخصصة في الأمان الإلكتروني يمكن أن يسهم بشكل كبير في تعزيز الأمان الإلكتروني بين الأفراد.

في الختام، يعكس هذا الجدول أهمية التركيز على تعزيز الأمان الإلكتروني بين جميع الفئات العمرية نظرًا لارتفاع معدل مداومتهم على التجوال في الحقل المعلوماتي، مما يتطلب تدخلات تعليمية وتوعوية مستمرة وفعالة.

14جدول رقم (14) يبين العلاقة بين الفئة العمرية للمبحوثين والتصريح بالهدية إلكترونيا

التصريح بالهدية لفئة العمرية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
من 18 21	6	8.6%	15	%20	21	30%
اكثر من 21سنة	35	%50	14	%21.4	49	70%
المجموع	41	58.6%	29	%20	70	%100

يتناول الجدول رقم 14 العلاقة بين الفئة العمرية للمبحوثين ومدى تصريحه بالهدية إلكترونياً. يوضح الجدول توزيع المبحوثين حسب الفئة العمرية وحالة التصريح بالهدية، مما يساعد في فهم تأثير العمر على هذا السلوك.

1. تحليل البيانات

أولاً: الفئة العمرية من 18 إلى 21 سنة:

– نعم (تصريح بالهدية): 8.6% من المبحوثين في هذه الفئة العمرية يصرحون بالهدية إلكترونياً.

– لا (عدم التصريح بالهدية): 21.4% من المبحوثين في هذه الفئة العمرية لا يصرحون بالهدية إلكترونياً.

– المجموع: 30% من المبحوثين هم من الفئة العمرية من 18 إلى 21 سنة.

ثانياً: الفئة العمرية أكثر من 21 سنة:

– نعم (تصريح بالهدية): 50% من المبحوثين في هذه الفئة العمرية يصرحون بالهدية إلكترونياً.

– لا (عدم التصريح بالهدية): 20% من المبحوثين في هذه الفئة العمرية لا يصرحون بالهدية إلكترونياً.

– المجموع: 70% من المبحوثين هم من الفئة العمرية أكثر من 21 سنة.

ثالثاً: العلاقة بين الفئة العمرية والتصريح بالهدية إلكترونياً:

– نعم (تصريح بالهدية): 58.6% من المبحوثين يصرحون بالهدية إلكترونياً.

– لا (عدم التصريح بالهدية): 41.4% من المبحوثين لا يصرحون بالهدية إلكترونياً.

القرار والتوصيات

القرار:

بناءً على البيانات، يتضح أن الأفراد في الفئة العمرية أكثر من 21 سنة يميلون بشكل أكبر إلى التصريح بالهدية إلكترونياً مقارنة بالفئة العمرية من 18 إلى 21 سنة.

التوصيات:

1. تعزيز الوعي بالأمان الإلكتروني: نظراً لأن نسبة كبيرة من الأفراد يصرحون بالهدية إلكترونياً، ينبغي تعزيز الوعي بالأمان الإلكتروني لحمايتهم من الاحتيال.

2. برامج توعية موجهة: تطوير برامج توعية موجهة لكل فئة عمرية، مع التركيز على الفئة العمرية أكثر من 21 سنة نظرًا لنشاطهم المرتفع في التصريح بالهدية.

3. تشجيع الممارسات الآمنة: تشجيع الأفراد على تبني ممارسات آمنة عند التصريح بالهدية إلكترونياً من خلال ورش عمل وحملات توعية.

4. توفير أدوات حماية: تطوير أدوات حماية متقدمة وسهلة الاستخدام لمساعدة الأفراد في حماية معلوماتهم عند التصريح بالهدية إلكترونياً.

5. التعاون مع منصات التجارة الإلكترونية: التعاون مع منصات التجارة الإلكترونية لتوفير إرشادات وتوجيهات حول كيفية التصريح بالهدية بأمان.

3. النتائج

– نشاط مرتفع بين الأكبر سنًا: الأفراد في الفئة العمرية أكثر من 21 سنة هم الأكثر تصريحاً بالهدية إلكترونياً بنسبة 50%.

– حاجة للتوعية المستمرة: الحاجة لتوعية مستمرة لجميع الفئات العمرية، حيث أن نسبة التصريح بالهدية إلكترونياً مرتفعة بشكل عام.

– دور المؤسسات: المؤسسات يمكن أن تلعب دورًا مهمًا في تعزيز الأمان الإلكتروني بين الأفراد من جميع الفئات العمرية.

4. الاستنتاجات

– تأثير العمر على التصريح بالهدية: العمر له تأثير واضح على السلوك المتعلق بالتصريح بالهدية إلكترونياً، مع زيادة النسبة بين الأفراد الأكبر سنًا.

– أهمية التوعية الشاملة: من الضروري توفير توعية شاملة ومستمرة لجميع الفئات العمرية لضمان حماية معلوماتهم أثناء التصريح بالهدية إلكترونياً.

– التعاون المؤسسي: التعاون بين المؤسسات التعليمية ومنصات التجارة الإلكترونية يمكن أن يسهم بشكل كبير في تعزيز الأمان الإلكتروني بين الأفراد.

في الختام، يعكس هذا الجدول أهمية التركيز على تعزيز الأمان الإلكتروني بين جميع الفئات العمرية نظرًا لارتفاع معدل التصريح بالهدية إلكترونياً، مما يتطلب تدخلات تعليمية وتوعوية مستمرة وفعالة.

الفرضية الثالثة

15جدول رقم (15) يبين رأي المبحوثين في الغاية من الاختراق:

غاية الاختراق	ك	%
سرقة المعلومات	29	%41,4
معلومات أخرى	41	%58,6
المجموع	70	%100

يتناول الجدول رقم 15 آراء المبحوثين حول الغاية من الاختراق الإلكتروني. يوضح الجدول توزيع الآراء بين المبحوثين حول الأسباب الرئيسية التي يعتقدون أنها وراء عمليات الاختراق الإلكتروني، مما يساعد في فهم الأسباب الرئيسية للاختراقات من وجهة نظر المستخدمين.

1. تحليل البيانات

أولاً: سرقة المعلومات:

- عدد المبحوثين: 29 مبحوث يعتقدون أن الغاية من الاختراق هي سرقة المعلومات.

- النسبة المئوية: 41.4% من إجمالي المبحوثين يرون أن الهدف الأساسي من الاختراق هو سرقة المعلومات.

ثانياً: معلومات أخرى:

- عدد المبحوثين: 41 مبحوث يعتقدون أن هناك أسبابًا أخرى للاختراق غير سرقة المعلومات.

- النسبة المئوية: 58.6% من إجمالي المبحوثين يرون أن هناك أغراض أخرى للاختراق.

ثالثاً: المجموع:

- عدد المبحوثين الكلي: 70 مبحوث.

- النسبة المئوية الكلية: 100%.

القرار والتوصيات

القرار:

تظهر البيانات أن معظم المبحوثين يعتقدون أن هناك أغراضًا أخرى للاختراق غير سرقة المعلومات. إلا أن نسبة كبيرة من المبحوثين (41.4%) يرون أن سرقة المعلومات هي الغاية الرئيسية.

التوصيات:

1. تعزيز الوعي بالأغراض المختلفة للاختراق: يجب على المستخدمين أن يكونوا على دراية بأن الاختراقات الإلكترونية يمكن أن تحدث لأسباب متنوعة وليس فقط لسرقة المعلومات.

2. تطوير برامج توعية شاملة: برامج توعية شاملة تشمل جميع الأغراض المحتملة للاختراق وكيفية الوقاية منها.

3. تعزيز الأمان الإلكتروني: تعزيز الأمان الإلكتروني لحماية جميع أنواع البيانات والمعلومات الحساسة.

4. التعاون مع الجهات المختصة: التعاون مع الجهات المختصة لتطوير استراتيجيات لمكافحة جميع أنواع الاختراقات الإلكترونية.

5. إجراء دراسات مستمرة: إجراء دراسات مستمرة لفهم الأسباب المتغيرة والدوافع وراء الاختراقات الإلكترونية.

3. النتائج

– تنوع الدوافع: الدوافع وراء الاختراقات الإلكترونية متنوعة، حيث يعتقد 58.6% من المبحوثين أن هناك أسبابًا أخرى غير سرقة المعلومات.

– أهمية التوعية: ضرورة توعية المستخدمين بأن الاختراقات يمكن أن تكون لها أهداف متعددة.

– حاجة لتعزيز الأمان الإلكتروني: أهمية تعزيز الأمان الإلكتروني لمواجهة جميع أنواع التهديدات.

4. الاستنتاجات

– الأسباب المتعددة للاختراق: من الواضح أن الأسباب وراء الاختراقات الإلكترونية متعددة وتتنوع بين سرقة المعلومات وأغراض أخرى.

– التوعية الشاملة: ضرورة توفير توعية شاملة للمستخدمين حول جميع الأغراض المحتملة للاختراق وكيفية الوقاية منها.

– تعزيز الحماية: تعزيز الأمان الإلكتروني لحماية المستخدمين من جميع أنواع الاختراقات الإلكترونية.

في الختام، يعكس هذا الجدول أهمية فهم وتوعية المستخدمين بالأسباب المختلفة للاختراقات الإلكترونية، مما يتطلب تعزيز الجهود التعليمية والأمنية لمكافحة هذه التهديدات المتنوعة.

16جدول رقم (16) يبين رأي المبحوثين من المتسبب في الاختراق:

سبب الاختراق	ك	%
الضحية	28	%40
الجاني	42	%60
المجموع	70	100%

يعكس جدول رقم (16) رأي المبحوثين حول من هو المتسبب في الاختراقات الإلكترونية، حيث يقدم البيانات المتعلقة بنسبة المبحوثين الذين يعتبرون أن الضحية أو الجاني هو المسؤول عن الاختراقات. يتناول هذا التحليل العميق الجوانب الإحصائية والبيانية، مع تقديم استنتاجات وتوصيات متعلقة بالسياق الأوسع للدراسة حول الوعي الأمني والجريمة الإلكترونية في المجتمع الجزائري.

1. تحليل البيانات

1. الضحية كمسبب للاختراق:

– يشير 40% من المبحوثين إلى أن الضحية تتحمل المسؤولية عن الاختراقات. يمكن تفسير هذا الرأي بعدة طرق:

– قلة الوعي الأمني: قد يكون هناك نقص في المعرفة الكافية بالطرق الوقائية لتجنب الاختراقات.

– إهمال الإجراءات الأمنية: يمكن أن يكون الإهمال في اتباع الممارسات الأمنية الجيدة سبباً في التعرض للاختراقات.

2. الجاني كمسبب للاختراق:

– يعتقد 60% من المبحوثين أن الجاني هو المسؤول الرئيسي عن الاختراقات. هذا يشير إلى وعي بوجود نوايا خبيثة وسلوكيات إجرامية تستهدف الضحايا.

– التطور التقني للجريمة الإلكترونية: تعكس هذه النسبة الفهم بأن التقنيات المتطورة والأساليب المتجددة للجناة تلعب دوراً رئيسياً في نجاح الاختراقات.

– استغلال الثغرات: يُظهر هذا الإدراك أن الجناة يستغلون نقاط الضعف في الأنظمة الأمنية لتحقيق أهدافهم.

2. القرار والتوصيات

بناءً على التحليل السابق، يمكن اقتراح مجموعة من التوصيات لتحسين مستوى الأمن وتقليل الاختراقات:

1. رفع مستوى الوعي الأمني:

– تنظيم ورش عمل ودورات تدريبية تهدف إلى زيادة الوعي الأمني بين جميع فئات المجتمع، خصوصاً حول الممارسات الجيدة لحماية البيانات الشخصية والشركات.

– تطوير برامج توعية مستمرة تعزز المعرفة بالتهديدات الإلكترونية وأساليب الحماية منها.

2. تعزيز الأنظمة الأمنية:

– ضرورة تحديث الأنظمة الأمنية بشكل دوري لضمان توفير أحدث الحمايات ضد الهجمات الإلكترونية.

– تطبيق سياسات أمنية صارمة في المؤسسات والشركات، بما في ذلك استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية.

3. تشجيع الإبلاغ عن الجرائم الإلكترونية:

– تشجيع الضحايا على الإبلاغ عن أي محاولات اختراق أو جرائم إلكترونية لتعزيز قدرة الجهات المختصة على التعامل مع هذه الجرائم بفعالية.

– تطوير قنوات تواصل مباشرة وسهلة بين الضحايا والجهات الأمنية المختصة.

4. البحث والتطوير في مجال الأمن الإلكتروني:

– دعم الأبحاث والدراسات المتعلقة بالأمن الإلكتروني للابتكار في تطوير أدوات وتقنيات جديدة لمكافحة الجريمة الإلكترونية.

– التعاون مع مؤسسات أكاديمية ومراكز بحثية لتطوير حلول أمنية متقدمة ومناسبة للسياق المحلي.

3. النتائج والاستنتاجات

من خلال تحليل جدول رقم (16) يتضح أن هناك إدراكاً متبايناً لمسؤولية الاختراقات بين الضحايا والجناة. تبرز النتائج أن الجزء الأكبر من المسؤولية يُلقى على الجاني (60%)، مما يشير إلى اعتراف واضح بالدور الهجومي والنوايا الخبيثة التي يمارسها الجناة في استهداف الضحايا.

في الوقت ذاته، لا يمكن إغفال نسبة الـ 40% التي تشير إلى أن الضحية قد تكون مسؤولة عن تعرضها للاختراق، مما يعكس أهمية الوعي الأمني ودوره في الوقاية من الجرائم الإلكترونية.

يتطلب التصدي للجريمة الإلكترونية مقاربة شاملة تجمع بين زيادة الوعي الأمني وتعزيز الأنظمة الأمنية وتطوير سياسات فعالة لمكافحة هذه الجرائم. توجيه جهود التوعية والتدريب المستمر للمجتمع، وتطوير البنية التحتية للأمن الإلكتروني، وتعزيز التعاون بين الجهات الحكومية والخاصة، يمكن أن يكون له تأثير كبير في تقليل معدلات الاختراقات وتحقيق بيئة إلكترونية آمنة للجميع.

17جدول رقم (17) يبين رأي المبحوثين في الغاية من الحسابات الوهمية:

غاية الحسابات الوهمية	ك	%
لغرض التمويه	13	%18,6
غرض الحماية	35	%50
أغراض أخرى	22	31.4%
المجموع	70	%100

يعرض جدول رقم (17) رأي المبحوثين حول الغايات التي تُستخدم من أجلها الحسابات الوهمية. يوضح الجدول التوزيع النسبي للمبحوثين بين الأغراض المختلفة، وهي التمويه، الحماية، وأغراض أخرى. سيتناول هذا التحليل العميق الجوانب الإحصائية والبيانية، مع تقديم استنتاجات وتوصيات متعلقة بالسياق الأوسع للدراسة حول الوعي الأمني والجريمة الإلكترونية في المجتمع الجزائري.

1. تحليل البيانات

1. استخدام الحسابات الوهمية لغرض التمويه:

- النسبة: 18.6%

- التفسير: يشير هذا الاستخدام إلى أن جزءاً من المبحوثين يعتمدون على الحسابات الوهمية لأغراض التمويه والخداع. قد يكون هذا مرتبطاً بأنشطة غير قانونية أو محاولة إخفاء الهوية لأسباب مختلفة، مثل التحايل أو التلاعب في العلاقات الاجتماعية أو التجارية.

2. استخدام الحسابات الوهمية لغرض الحماية:

- النسبة: 50%

- التفسير: تُعتبر هذه الفئة الأكبر بين المبحوثين، مما يشير إلى أن نصف العينة يستخدم الحسابات الوهمية كوسيلة لحماية الخصوصية أو تجنب التهديدات الإلكترونية. يمكن أن يتضمن ذلك حماية المعلومات الشخصية، تجنب التتبع، أو الحفاظ على الأمن الشخصي ضد الهجمات الإلكترونية.

3. استخدام الحسابات الوهمية لأغراض أخرى:

- النسبة: 31.4%

- التفسير: تشير هذه النسبة إلى وجود دوافع متنوعة أخرى لاستخدام الحسابات الوهمية، قد تشمل أسباباً اجتماعية أو تجارية أو حتى ترفيهية. يمكن أن يتضمن ذلك استخدام الحسابات الوهمية لمراقبة الآخرين، الوصول إلى محتوى محظور، أو المشاركة في مجتمعات إلكترونية دون الكشف عن الهوية الحقيقية.

2. القرار والتوصيات

بناءً على التحليل السابق، يمكن تقديم مجموعة من التوصيات لتحسين الوعي الأمني وتوجيه استخدام الحسابات الوهمية بشكل صحيح وآمن:

1. تعزيز التوعية حول الاستخدام الآمن للحسابات الوهمية:

– تنظيم حملات توعية توضح الأغراض المشروعة لاستخدام الحسابات الوهمية وكيفية استخدامها بشكل آمن دون انتهاك القانون أو حقوق الآخرين.

– تقديم معلومات حول المخاطر المرتبطة بالاستخدام غير المشروع للحسابات الوهمية وكيفية تجنبها.

2. توفير أدوات وموارد لحماية الخصوصية:

– تطوير وتقديم أدوات تكنولوجية تساعد الأفراد على حماية خصوصيتهم دون الحاجة لاستخدام الحسابات الوهمية.

– تشجيع استخدام برامج وتطبيقات أمنية تتيح للمستخدمين حماية معلوماتهم الشخصية بفعالية.

3. إعداد سياسات وإجراءات قانونية:

– تعزيز الإطار القانوني لمكافحة الاستخدام غير المشروع للحسابات الوهمية، مع توضيح العواقب القانونية لمثل هذه الأنشطة.

– تشجيع التعاون بين الجهات الحكومية والخاصة لمراقبة ومكافحة الجرائم الإلكترونية المرتبطة بالحسابات الوهمية.

4. تطوير برامج دعم نفسي واجتماعي:

– توفير دعم نفسي واجتماعي للأفراد الذين يستخدمون الحسابات الوهمية لأسباب تتعلق بالخوف أو القلق، وذلك لمساعدتهم على التعامل مع مشاكلهم بطرق أكثر أماناً وفعالية.

3.النتائج والاستنتاجات

من خلال تحليل جدول رقم (17)، يتضح أن الحسابات الوهمية تُستخدم لأغراض متنوعة، تتراوح بين التمويه والحماية إلى أغراض أخرى غير محددة. يبرز الاستخدام لأغراض الحماية كنسبة الأعلى، مما يعكس قلقاً واسعاً بين المبحوثين بشأن حماية الخصوصية والأمان الشخصي.

تعتبر هذه النتائج مؤشراً مهماً على ضرورة تعزيز الجهود التوعوية والتقنية والقانونية لحماية المستخدمين في الفضاء الإلكتروني، وتشجيع الاستخدام الآمن والمسؤول للتكنولوجيا.

يعكس تنوع آراء المبحوثين حول غايات استخدام الحسابات الوهمية الحاجة إلى استراتيجيات متكاملة تجمع بين التوعية والحماية القانونية والتقنية. توجيه الجهود نحو تعزيز الوعي الأمني ودعم الخصوصية يمكن أن يساهم في تقليل المخاطر المرتبطة بالاستخدام غير المشروع للحسابات الوهمية، وتحقيق بيئة إلكترونية أكثر أماناً وموثوقية لجميع المستخدمين.

18جدول رقم (18) يبين العلاقة بين إتقان استعمال الوسائط التكنولوجية الرأي في قلة وعي مستعملي الوسائط في المجتمع الجزائري

قلة الوعي / استعمال الوسائط التكنولوجية	نعم		لا		المجموع	
	ك	%	ك	%	ك	%
جيد	7	10%	8	%11.4	15	%21.4
حسن	13	18.6%	7	%10	20	%28.6
متوسط	6	8.6%	14	%20	20	%28.6
ضعيف	15	%21.4	0	%00	15	%21.4
المجموع	28	%58.6	29	%41.4	70	%100

يعرض جدول رقم (18) العلاقة بين إتقان استعمال الوسائط التكنولوجية والرأي في قلة وعي مستعملي هذه الوسائط في المجتمع الجزائري. يوضح الجدول توزيع آراء المبحوثين حول قلة الوعي بناءً على مستوى إتقانهم للوسائط التكنولوجية. سيتناول هذا التحليل العميق الجوانب الإحصائية والبيانية، مع تقديم استنتاجات وتوصيات متعلقة بالسياق الأوسع للدراسة حول الوعي الأمني والجريمة الإلكترونية في المجتمع الجزائري.

1. تحليل البيانات

1. إتقان الوسائط التكنولوجية بشكل جيد:

- قلة الوعي نعم: 7 مبحوثين يمثلون 10% من إجمالي العينة.
- قلة الوعي لا: 8 مبحوثين يمثلون 11.4% من إجمالي العينة.

– التفسير: يشير هذا إلى أن الذين يتقنون استعمال الوسائط التكنولوجية بشكل جيد لديهم وجهات نظر متباينة حول قلة الوعي، حيث أن نسبة كبيرة منهم لا يرون مشكلة في قلة الوعي.

2. إتقان الوسائط التكنولوجية بشكل حسن:

– قلة الوعي نعم: 13 مبحوثين يمثلون 18.6%.

– قلة الوعي لا: 7 مبحوثين يمثلون 10%.

– التفسير: يعتقد جزء كبير ممن يمتلكون إتقانًا حسنًا للوسائط التكنولوجية بوجود مشكلة في قلة الوعي بين مستعملي الوسائط، مما قد يعكس خبرتهم ومعرفتهم بالمخاطر المرتبطة بالاستخدام غير الواعي.

3. إتقان الوسائط التكنولوجية بشكل متوسط:

– قلة الوعي نعم: 6 مبحوثين يمثلون 8.6%.

– قلة الوعي لا: 14 مبحوثين يمثلون 20%.

– التفسير: الفئة التي تمتلك إتقانًا متوسطًا ترى بشكل أكبر عدم وجود مشكلة في قلة الوعي، مما قد يعكس قلة اطلاعهم على الجوانب الأمنية والمخاطر المرتبطة بالوسائط التكنولوجية.

4. إتقان الوسائط التكنولوجية بشكل ضعيف:

– قلة الوعي نعم: 15 مبحوثين يمثلون 21.4%.

– قلة الوعي لا: 0 مبحوثين.

– التفسير: كل الذين لديهم إتقان ضعيف يرون أن هناك مشكلة في قلة الوعي، مما يعكس بشكل كبير عدم معرفتهم الكافية واستخدامهم للوسائط التكنولوجية بشكل غير صحيح.

2. القرار والتوصيات

بناءً على التحليل السابق، يمكن تقديم مجموعة من التوصيات لتحسين الوعي الأمني وزيادة كفاءة استعمال الوسائط التكنولوجية في المجتمع الجزائري:

1. تعزيز التعليم والتدريب على الوسائط التكنولوجية:

– تنظيم برامج تدريبية للمستخدمين من مختلف الأعمار والمستويات التعليمية لتحسين مهاراتهم في استخدام الوسائط التكنولوجية.

– تقديم دورات متخصصة في الأمان الرقمي لتعريف المستخدمين بالممارسات الصحيحة لتجنب الاختراقات والأضرار الإلكترونية.

2. نشر الوعي حول المخاطر التكنولوجية:

– تنظيم حملات توعية واسعة النطاق توضح المخاطر المرتبطة بالاستخدام غير الواعي للوسائط التكنولوجية وكيفية تجنبها.

– استخدام وسائل الإعلام المختلفة لتسليط الضوء على أهمية الوعي الرقمي وتأثيره على الأمن الشخصي والاجتماعي.

3. دعم الأبحاث والدراسات في مجال الأمان الرقمي:

– تشجيع الأبحاث والدراسات المتعلقة بتحديد أفضل الممارسات في استخدام الوسائط التكنولوجية بأمان.

– تطوير شراكات بين المؤسسات الأكاديمية والشركات التقنية لإيجاد حلول عملية للتحديات الأمنية الرقمية.

4. تشجيع الاستخدام المسؤول للوسائط التكنولوجية:

– تطوير برامج توعية في المدارس والجامعات لتشجيع الشباب على الاستخدام المسؤول للوسائط التكنولوجية.

– توفير موارد تعليمية وإرشادية للمستخدمين حول كيفية حماية معلوماتهم الشخصية والبيانات الحساسة.

3. النتائج والاستنتاجات

من خلال تحليل جدول رقم (18)، يتضح أن هناك تفاوتًا في وجهات نظر المبحوثين حول قلة الوعي بين مستعملي الوسائط التكنولوجية بناءً على مستوى إتقانهم لهذه الوسائط. الفئات ذات الإتقان الجيد والمتوسط تعبر بشكل أكبر عن عدم وجود مشكلة كبيرة في قلة الوعي، في حين أن الفئات ذات الإتقان الضعيف تعترف بوجود مشكلة كبيرة في قلة الوعي.

يعكس هذا التحليل الحاجة الملحة لتعزيز التعليم والتدريب في مجال الوسائط التكنولوجية وزيادة الوعي بالأمان الرقمي في المجتمع الجزائري. إن تعزيز المهارات والمعرفة الرقمية يمكن أن يساهم بشكل كبير في تقليل المخاطر الأمنية وزيادة الاستفادة من التقنيات الحديثة بأمان وفعالية.

الخاتمة العامة

الخاتمة العامة

في ضوء النتائج المستخلصة من هذه الدراسة، يمكن القول إن الوعي الأمني في المجتمع الجزائري يعاني من قصور واضح، مما يسهم في انتشار الجرائم المعلوماتية. وقد أظهرت النتائج أن هناك تفاوتًا كبيرًا في مستويات الوعي الأمني بين الأفراد، حيث يلعب المستوى التعليمي والبيئة الجغرافية دورًا حاسمًا في تحديد مستوى الوعي.

من خلال تحليل الجداول والإحصاءات، تبين أن الفئات الأكثر عرضة للجرائم المعلوماتية هي تلك التي تفتقر إلى المعرفة التقنية والوعي الأمني. كما أظهرت الدراسة أن الحسابات الوهمية تُستخدم بشكل كبير لأغراض الحماية والتمويه، مما يشير إلى وجود مخاوف حقيقية بين الأفراد تجاه الجرائم المعلوماتية.

الاقتراحات والتوصيات

1. تعزيز برامج التوعية الأمنية :يجب تنظيم حملات توعية شاملة تستهدف جميع فئات المجتمع، مع التركيز على الفئات الأقل وعيًا تقنيًا.
2. تطوير المناهج التعليمية :تضمين موضوعات الأمن السيبراني في المناهج الدراسية لجميع المراحل التعليمية لزيادة الوعي بين الأجيال الجديدة.
3. توفير دورات تدريبية :تقديم دورات تدريبية مجانية عبر الإنترنت لتعليم الأفراد كيفية حماية بياناتهم الشخصية وتجنب الوقوع ضحايا للجرائم المعلوماتية.
4. تفعيل القوانين والتشريعات :ضرورة تحديث وتفعيل القوانين المتعلقة بالجرائم المعلوماتية لردع المجرمين وحماية الأفراد والمؤسسات.

الاستنتاج العام

خلصت الدراسة إلى أن هناك حاجة ماسة لزيادة الوعي الأمني بين أفراد المجتمع الجزائري. إن تطوير البرامج التعليمية والتدريبية، بالإضافة إلى تفعيل القوانين الصارمة، سيسهم بشكل كبير في الحد من انتشار الجرائم المعلوماتية. كما أن التعاون بين الجهات الحكومية والمؤسسات التعليمية والاجتماعية يعد ضروريًا لتحقيق هذا الهدف.

في النهاية، يمكن القول إن معالجة قضية الجرائم المعلوماتية تتطلب جهودًا مشتركة من جميع أفراد المجتمع، مع التركيز على التعليم والتوعية المستمرة لحماية الأفراد والمؤسسات من مخاطر هذه الجرائم.

قائمة المراجع

قائمة المراجع

قائمة المراجع:

إبراهيم عبد الرحمن، دور الشرطة في مجال تنمية الوعي الأمني لدى الجماهير، كلية الدراسات العليا ،2003.

ابن منظور، ج.د (1978)، لسان العرب بيروت، دار صادر.

أبو بكر أحمد همام عبد المجيد ، أثار الجرائم المعلوماتية وسبل مكافحتها ، الوادي 2020

أبو جادو، سيكولوجية التنشئة الاجتماعية ، الأردن ، دار المسيرة ، 2006.

أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، مصر ،2005.

أسماء بنت عبد الله بن عبد المحسن التويجري ، الخصائص الاجتماعية والاقتصادية للعائدات للجريمة، جامعة نايف العربية للعلوم الأمنية ، السعودية، 2011.

بوعناد فاطمة زهرة ، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول ، 2013.

تركي بن عبد الله ، تصور استراتيجي لتنمية الوعي الأمني للتعامل مع الآخرين ، دراسة الحالة، السعودية 2021.

تركي بن عبد الله، تصور استراتيجي لتنمية الوعي الأمني للتعامل مع الآخرين ، دراسة الحالة ، كلية العلوم الإستراتيجية، السعودية، 2021.

جابر ضرغام (2017)،جريمة التجسس المعلوماتي دراسة مقارنة ، جمهورية مصر العربية ، المركز العربي للدراسات والبحوث العلمية.

جابر، ضرغام، جريمة التجسس المعلوماتي "دراسة مقارنة" ، جمهورية مصر العربية ، المركز العربي للدراسات والبحوث العلمية، 2017.

جامعة محمد خيضر .2013 ، ص 10 أمينة دير ،أثر التهديدات البيئة على واقع الأمن الإنساني في إفريقيا دراسة حالة،

الجريمة الافتراضية الملتقى الدولي التنظيم القانوني للانترنت و الجريمة الالكترونية ، الجلفة ، الجزائر 2009 دياب البداينة

جودة بن جابر ، علم النفس الاجتماعي، دار الثقافة، الأردن.

خالد ممدوح ، أمن الجريمة الالكترونية ، الدار الجامعة إسكندرية 2008.

دراسة مقارنة في التشريعات العربية و الأجنبية ، الرياض ،2014 ، ص 09 أيمن عبد الله فكري ، الجرائم المعلوماتية

دياب،ف (1978)، نمو الطفل وتنشئته بين الأسرة ودور الحضانة، مصر، مكتبة النهضة العربية.

ذياب الرشيد ، ناصر الصالح،فحص النظرية العامة للجريمة في المملكة العربية السعودية ، المجلد 20، العدد 1

زين العابدين درويش ، علم النفس الاجتماعي أسسه و تطبيقاته، دار الفكر العربي ، القاهرة ، مصر .

شريف، ع (2004)، التنشئة الاجتماعية للطفل في عصر العولمة ، مصر ،دار الفكر العربي.

الصالحي، عبد المحس، الوعي الأمني ودوره في حياتنا اليومية، الرياض ، مطابع العصر 2005.

طارق إبراهيم دسوقي عطية، الأمن ألمعلوماتي، دار جامعة جديدة 2015.

عبد الله بن عباس، علم الاجتماع التربوي، المكتب الجامعي الحديث، الإسكندرية، مصر 2002.

العمري ،عبد الله بن محمد ، دور الثقافة الأمنية في الوقاية من الفكر المتطرف في المجتمع السعودي، الرياض 2014.

فاروق مداس ، قاموس مصطلحات علم الاجتماع ، الجزائر ، دار مدني للطباعة والنشر، 2003.

قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

المادة 394 مكرر 5 والمادة 394 مكرر 7 من قانون العقوبات الجزائري

المادة 394مكرر 4 من قانون العقوبات الجزائري

محمد بن عودة، النظريات المعاصرة للجريمة والانحراف، جامعة الجيلالي بونعامة خميس مليانة، 2016-2017.

محمد عبد الله أبو بكر، موسوعة جرائم معلوماتية، المكتب العربي الحديث، الإسكندرية، 2011.

محمد عمارة، مقومات الأمن الاجتماعي في الإسلام،القاهرة،مصر، مكتبة الإمام البخاري، الطبعة الأولى ،2009.

منى شاكر فراج العبسلي، تأثير الجريمة الالكترونية على النواحي الاقتصادية ، كانون أونلاين ،2020.

هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية،القاهرة 1992.

هرندي.ك. مؤسسات التنشئة الاجتماعية بين الأساليب و العوائق، العائلة و المدرسة، مجلة الحوار الثقافي 02 .

هشام بشير،2012، الآليات الدولية لمكافحة الجريمة الالكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية

هشام محمد فريد رستم، عقوبات و مخاطر جرائم معلوماتية، دار النهضة العربية ، القاهرة ، 2000.

هلال نصار، إنعكاسات الجرائم الالكترونية على المجتمع ورؤية قانونية ، 2022.

يحي خير الله عودة ، مجلة الآداب ، البيئة والسلوك الإجرامي(دراسة نظرية في الإنثروبولوجيا الجنائية، الجامعة المستنصرية.

قائمة الملاحق

قائمة الملاحق

الاستمارة

المعلومات الشخصية:

1_ الفئة العمرية (21.18)(21 فما فوق)

2_ الجنس: ذكر أنثى

3_ المستوى الجامعي (ليسانس- ما ستر)

4_ البيئة الجغرافية (ريفي- حضري)

المحور الأول: مدى استكمال التكنولوجيا ودوره في التعرض للجريمة المعلوماتية

1_ هل لديك حسابات في مواقع التواصل الاجتماعي: نعم لا

ما نوع هذه الحسابات : فايسبوك

انستغرام

أخرى اذكرها

2_ كم لديك من حساب 1_2_3_4

3_ هل لديك حسابات وهمية؟ نعم لا

لماذا

4_هل انت مداوم على التجوال في الحقل ألمعلوماتي؟ نعم لا

5_ هل تتقن جيدا استعمال لمواقع التواصل الاجتماعي و الوسائط الالكترونية: جبد حسن متوسط ضعيف

6_ هل تعرضت يوما إلى الاختراق الالكتروني ؟ نعم لا

7_ لماذا في رأيك تعرضت له:

نقص الحماية

قوة الشخص المخترق

المحور الخاص: بالوعي بالحماية الالكترونية؟

1_هل تصرح بهويتك الكترونيا؟ نعم لا

2_ لماذا تقوم بذلك؟ تراه أمر عادي

لعدم اهتمامك بالاختراق

3_ عل ترى أن الاختراق الالكتروني يشكل عائق في مجتمعنا أم لا ؟ نعم لا

4 لماذا؟

5_ هناك بعض الأشخاص يستعملون حسابات وهمية

6_ لماذا ؟ لغرض التمويه

لغرض الحماية

أخرى حددها

7_ هل تخاف الاختراق الالكتروني: نعم لا

8_ لماذا؟

9_ في حالة التعرض الاختراق الالكتروني هل تبلغ عن ذلك ؟ نعم لا

10 لماذا ؟

11_ هل ترى أن الاختراق غايته سرقة المعلومات أم أشياء أخرى؟

سرقة المعلومات

معلومات أخرى

12_ هل ترى أن الاختراق بسببه:

الضحية

الجاني

13_ لماذا في رأيك ؟

14_ هل ترى أن هناك قلة وعي أمني لدى الأشخاص المستعملين للوسائط الاجتماعية في مجتمعنا؟

نعم لا

١

الاستمارة

المعلومات الشخصية

1- الفئة العمرية (18،21) (21 فما فوق)

2- الجنس: ذكر انثى

3- المستوى الجامعي (ليسانس ماستر)

4- البيئة الجغرافية (ريفي حضري)

المحور الأول: مدى استكمال التكنولوجيا ودوره في التعرض الى الجريمة الالكترونية

1- هل لديك حسابات في مواقع التواصل الاجتماعي:؟ نعم لا

ما نوع هذه الحسابات: - فايسبوك

- انستغرام

غيرها اذكرها TIK TOK

2- كم لديك من حساب؟ 1-/2-/3/-4-3)

3- هل لديك حسابات وهمية؟ نعم لا

لماذا؟ ليس لدي وقت

4- هل انت مداوم على التجوال في الحقل المعلوماتي؟ نعم لا

5- هل تتقن جيدا استعمال لمواقع التواصل الاجتماعي والوسائط التكنولوجية: جيد حسن متوسط ضعيف

6- هل تعرضت يوما الى الاختراق الالكتروني؟ نعم لا

7- لماذا في رايك تعرضت له:

- نقص الحماية

- قوة الشخص المخترق

المحور الخاص: بالوعي بالحماية الالكترونية؟

1- هل تصرح بهويتك الكترونيا؟ نعم لا

2- لماذا تقوم بذلك؟ - تراه امر عادي

- لعدم اهتمامك بالاختراق

3- هل ترى ان الاختراق الالكتروني يشكل عائق في مجتمعنا ام لا؟ نعم لا

4- لماذا؟ لأنه يسبب مشاكل لصاحب الحساب

5- هناك بعض الأشخاص يستعملون حسابات وهمية

6- لماذا؟ - لغرض التمويه

- لغرض الحماية

أخرى حددها

7- هل تخاف الاختراق الالكتروني: نعم لا

8- لماذا؟ لأنه يكشف أسرارك أو يريد منك ان تكشف

9- في حالة التعرض الاختراق الالكتروني هل تبلغ عن ذلك؟ نعم لا

10- لماذا؟ لكثرة الاجراءات

11- هل ترى ان الاختراق غايته سرقة معلومات ام أشياء أخرى؟

- سرقة معلومات

- معلومات أخرى

12 – هل ترى ان الاختراق بسببه:

- الضحية

- الجاني

13- لماذا في رأيك؟ لأنه هو من قام بعملية الاختراق

14- هل ترى ان هناك قلة وعي امني لدى الأشخاص المستعملين للوسائط الاجتماعية في مجتمعنا؟ نعم لا

الملخص

في العصر الرقمي الذي نعيشه اليوم، أصبح العالم أشبه بقرية صغيرة مترابطة عبر شبكة الإنترنت والتكنولوجيا الرقمية. يعتمد الأفراد والمؤسسات بشكل متزايد على التكنولوجيا في مختلف جوانب الحياة اليومية، سواء في العمل أو التعليم أو حتى الترفيه والتواصل الاجتماعي. ومع هذا الاعتماد المتزايد، ظهرت مخاطر جديدة تتعلق بأمن المعلومات، وأبرزها الجرائم المعلوماتية مثل سرقة الهوية، الاحتيال المالي، الهجمات الإلكترونية، والبرمجيات الخبيثة.

يعتبر الوعي الأمني خط الدفاع الأول والأهم ضد هذه الجرائم، حيث يشمل معرفة الأفراد بالمخاطر الأمنية المحتملة والإجراءات الوقائية التي يجب اتخاذها لحماية أنفسهم ومعلوماتهم الشخصية. في الجزائر، كما هو الحال في العديد من الدول، يشهد استخدام التكنولوجيا انتشارًا سريعًا مما يجعل الوعي الأمني قضية حيوية لحماية المجتمع من تهديدات الجرائم المعلوماتية.

على الرغم من الجهود المبذولة لتعزيز الوعي الأمني في الجزائر، لا تزال هناك فجوات كبيرة تؤدي إلى تعرض الأفراد والمؤسسات لمخاطر أمنية كبيرة. نقص التوعية والتدريب الكافي وضعف السياسات الأمنية وتدني مستوى الوعي.

الكلمات المفتاحية: الوعي الأمني، العصر الرقمي، الجريمة، المخاطر الأمنية، التكنولوجيا.

Abstract

In the digital age we live in today, the world has become akin to a small village interconnected through the internet and digital technology. Individuals and organizations increasingly rely on technology in various aspects of daily life, whether in work, education, entertainment, or social communication. With this growing dependence, new risks related to information security have emerged, most notably cybercrimes such as identity theft, financial fraud, cyber-attacks, and malware.

Security awareness is considered the first and most important line of defense against these crimes. It involves individuals' knowledge of potential security risks and the preventive measures that should be taken to protect themselves and their personal information. In Algeria,

as in many other countries, the rapid spread of technology makes security awareness a crucial issue to protect the community from the threats of cybercrimes.

Keywords : Digital Age, Security awareness, security risk, spread of technology.