وزارة التعليم العالي والبحث العلمي

جامعة وهران 2 –محمد بن أحمد–

كلية العلوم الاجتماعية

تخصص الجريمة والانحراف

مذكرة التخرج لنيل شهادة الماستر تخصص جريمة والانحراف

الجريمة الإلكترونية

من إعداد الطالبان:

خيرالدين سعيد

مسلم ياسين

تحت إشراف:

بوجملين نوال

لجنة المناقشة

الرقم	الأساتذة	الجامعة	الصفة
1	بن عاشور سالم	جامعة وهران 2	رئيسا
2	بوجملين نوال	جامعة وهران 2	مؤطر
3	مداني فواتيح صافية	جامعة وهران 2	مناقشا

السنة الجامعية:2024/2023

بسم الله والصلاة والسالم على سيدنا ونبينا وعلى من تبعه ومن ولاه الى يوم الدين اهدي ثمرة جهدي هذا المتواضع الى من قال فيهما الرحمان:" وقضى ربك الا تعبدوا إلا إياه وبالوالدين إحسانا"

الى من سهرت الليالي النعم بالراحة الى من ساندتني بدعوتها الى من كانت لي متبعا للحنان ورمزا للصبر.

الى امي الغالية حفضها وادام عليها الصحة والعافية.

خيرالدين سعيد

بسم الله والصلاة والسلام على أشرف المرسلين سيدنا محمد الصادق الأمين

إلى أمي الغالية.....

أهديك هذه المذكرة التي تمثل ثمرة جهدي وسعي نحو تحقيق أحلامي، إنك كنت دائما مصدر إلهامي ودعمي في كل خطوة خطوتها.

لقد علمتني أن العمل والمثابرة هما المفتاحان للنجاح، وكنت دائما تساندني في الأوقات الصعبة وأقدر كل لحظة قضيتها بجانبي وكل نصيحة قدمتها لي

تحياتي الخالصة.....

مسلم ياسين

ملخص الدراسة:

يتناول الفصل الأول نشأة الإطار المفاهيمي موضحًا كيف أصبحت هذه الجرائم تهديدًا متزايدًا في العصر الرقمي و يوضح الفصل الثاني منهجية البحث المستخدمة، حيث تم تحليل مختلف التعريفات المتعلقة بالجريمة المعلوماتية، مما يعكس تنوع المصطلحات والمفاهيم المرتبطة بها ويتناول الفصل الثالث نتائج الدراسة الميدانية، خاصة عبر مواقع التواصل الاجتماعي، واستعرض التحديات التي يواجهها هؤلاء الضحايا وتقدم الدراسة توصيات حول كيفية التصدي للجرائم الإلكترونية، بما في ذلك أهمية التوعية والتثقيف القانوني للأفراد والمجتمعات بشكل عام، تسلط الدراسة الضوء على أهمية فهم الجرائم الإلكترونية وتأثيرها على الأفراد والمجتمعات، وتدعو إلى اتخاذ إجراءات فعالة لمواجهتها.

تؤكد الدراسة على أن الجرائم الإلكترونية ليست مجرد سلوك فردي، بل هي نتيجة لتغيرات اجتماعية واقتصادية أوسع. لذا، يتطلب التصدي لها فهمًا عميقًا للسياق الاجتماعي الذي تحدث فيه.

وبزيادة الوعي العام حول مخاطر الجرائم الإلكترونية ووسائل الحماية الممكنة .كما تدعو إلى تطوير استراتيجيات تعليمية وتثقيفية لتعزيز فهم الأفراد لهذه الجرائم وكيفية التصدي لها.

الكلمات المفتاحية: الجريمة الالكترونية، الاجرام، الأنترنت، مواقع التواصل الاجتماعي.

Résumé :

Le premier chapitre traite de l'émergence du cadre conceptuel, expliquant comment ces crimes sont devenus une menace croissante à l'ère numérique. Le deuxième chapitre explique la méthodologie de recherche utilisée, où diverses définitions liées à la criminalité informatique ont été analysées, reflétant la diversité des termes. Et les concepts qui y sont associés. Le troisième chapitre traite des résultats de l'étude sur le terrain, en particulier sur la communication sociale, et passe en revue les défis auxquels sont confrontées ces victimes. L'éducation juridique pour les individus et les sociétés en général. L'étude souligne l'importance de comprendre la cybercriminalité et son impact sur les individus et les sociétés, et appelle à prendre des mesures efficaces pour y faire face. L'étude souligne que la cybercriminalité n'est pas seulement un comportement individuel, mais plutôt le résultat de changements sociaux et économiques plus vastes. Par conséquent, y remédier nécessite une compréhension approfondie du contexte social dans lequel il se produit. Et en sensibilisant le public aux dangers de la cybercriminalité et aux moyens de protection possibles. Il appelle également au développement de stratégies éducatives et éducatives pour améliorer la compréhension des individus sur ces crimes et sur la manière d'y faire face.

Mots-clés : cybercriminalité, criminalité, Internet, sites de réseaux sociaux.

الفهرس

قائمة الجداول:

الفصل الأول:
الاطار المنهجي

مقدمة:

تعتبر الجرائم الإلكترونية من أبرز التحديات التي تواجه المجتمعات الحديثة في عصر المعلومات والتكنولوجيا. مع التقدم السريع في تكنولوجيا المعلومات والاتصالات، أصبحت هذه الجرائم تشكل تهديدًا متزايدًا للأفراد والمؤسسات على حد سواء. تتنوع أشكال الجرائم الإلكترونية، بدءًا من الاحتيال عبر الإنترنت، وصولاً إلى سرقة الهوية والبيانات الشخصية، مما يتطلب استجابة فعالة من قبل الحكومات والمجتمعات.

تتجلى أهمية دراسة الجرائم الإلكترونية في كونها ظاهرة متفشية تتطلب فهمًا عميقًا لسمات ضحاياها وآليات التصدي لها. فمع تزايد استخدام منصات التواصل الاجتماعي والتجارة الإلكترونية، أصبح الأفراد أكثر عرضة للاحتياج إلى الحماية من هذه الجرائم. لذا، فإن البحث في هذا المجال يسهم في تطوير استراتيجيات فعالة للتوعية والتثقيف، مما يساعد على تقليل المخاطر المرتبطة بالجرائم الإلكترونية.

شهدت المجتمعات الحديثة تطورًا تكنولوجيًا سريعًا، ومع تزايد الاعتماد على الإنترنت والتكنولوجيا الرقمية، أصبحت الجرائم الإلكترونية تمثل تحديًا كبيرًا يتطلب اهتمامًا خاصًا من الأفراد والجهات الحكومية على حد سواء. تتنوع أشكال هذه الجرائم بشكل كبير، حيث تشمل الاحتيال عبر الإنترنت، والقرصنة، وسرقة الهوية، والابتزاز، مما يعكس الطبيعة المتطورة لهذه التهديدات.

تتناول هذه الدراسة منهجية شاملة لفهم الجرائم الإلكترونية، بدءًا من تعريفها وأنواعها، وصولاً إلى تحليل سمات ضحاياها. كما تسلط الضوء على أهمية تكوين دراسات مستفيضة حول هذا الموضوع، بهدف إيجاد حلول مناسبة للتصدي لهذه الظاهرة المتزايدة.

بناء الإشكالية:

يعيش العالم اليوم في أسمى مراحل تطوره التكنولوجي، وذلك بفضل الثورة المعلوماتية التي قربت البعيد وأزالت الفجوات الزمنية والمكانية. لقد أحدثت هذه الثورة تغييرات هائلة في جميع جوانب الحياة، خصوصاً في مجال الاتصالات وأنظمة المعلومات، حتى أصبح عصرنا يُعرف بعصر المعلومات. فالمعلومة أصبحت سيدة الموقف وضرورة أساسية في هذا العصر الحديث، وهي المحرك الرئيسي لأي تقدم إنساني في مختلف المجالات.

ساهمت تكنولوجيا الإعلام والاتصال في تسهيل العديد من الأمور التي كانت تتطلب جهدًا كبيرًا، وفتحت آفاقًا جديدة وفرصًا متزايدة لتحسين حياة الشعوب. كما ظهرت اختراعات عديدة خدمت الإنسان، وساهمت في تحقيق الرفاهية وتوفير الوقت والجهد والأمان. ولكن، فإن الاستخدام غير الصحيح لهذه التكنولوجيا الحديثة قد يؤدي إلى عواقب وخيمة.

في حين كانت تكنولوجيا الإعلام والاتصال في البداية نعمة للعالم، أصبحت اليوم تهديدًا للأمن البشري بسبب الاستعمال السلبي لها، خاصة في مجال الإنترنت والفضاء الرقمي. فقد برزت أنواع جديدة من الجرائم التي اكتسبت طابعًا عصريًا، مثل الاحتيال الإلكتروني، والذي يُعتبر من أبرز وأخطر هذه الجرائم، فهو يشير إلى صورة مستحدثة للاحتيال تقوم على إساءة استخدام الأجهزة الإلكترونية في نظم المعالجة للبيانات من أجل الحصول بغير حق على أموال أو أصول أو خدمات...

يتعرض الكثيرون لأساليب احتيالية على الإنترنت، مما يجعل من الضروري أن يكون الأفراد على دراية بمخاطر الاحتيال الإلكتروني وطرق حمايتهم منها. لذا، فإن الجرائم الإلكترونية بمختلف أشكالها وأنواعها أصبحت تشكل تحديًا كبيرًا يتطلب الحذر والتصدي الفعّال، ولذلك قمنا بطرح إشكالية التالية:

ماهي سمات ضحايا الجرائم الإلكترونية؟

دراسات سابقة:

1.دراسة محلية:

دراسة الدكتور بولحية شهيرة بالمركز الجامعي البريكة 01-12-2019 :

مقال بعنوان " الاحتيال الإلكتروني لمجلة دراسات القانونية والاقتصادية "

يركز المقال على تعريف هذه الجرائم، أشكالها، ووسائلها، بالإضافة إلى كيفية تأثيرها على الأمان المعلوماتي. كما يتناول المقال التحديات التي تواجه الأفراد في مواجهة هذه الجرائم، والتي يتم من خلالها طرحت السؤال التالي: ما هي طبيعة الاحتيال الإلكتروني، وما هي تأثيراته على الأفراد والمجتمعات، وكيف يمكن تعزيز الوعي والحماية ضد هذه الجرائم؟

المنهج المستخدم في هذا المقال يعتمد على منهجية تحليلية واستقرائية:

يبدأ المقال بتعريف المفاهيم الأساسية المتعلقة بالاحتيال الإلكتروني، مما يساعد في وضع إطار نظري لفهم الظاهرة.

استعراض الأدبيات :يتضمن المقال مراجعة للأبحاث والدراسات السابقة المتعلقة بالجرائم الإلكترونية، مما يعزز من فهم السياق التاريخي والتطورات في هذا المجال.

تحليل الحالات :يحتوي المقال تحليل حالات واقعية أو أمثلة على الاحتيال الإلكتروني، مما يساعد في توضيح كيفية حدوث هذه الجرائم وتأثيرها على الأفراد والمجتمعات.

تقديم الحلول :يستعرض المقال استراتيجيات ووسائل لمواجهة الاحتيال الإلكتروني، مما يعكس منهجًا تطبيقيًا يهدف إلى تقديم حلول عملية للمشكلات المطروحة.

التوجه الاستقرائي :من خلال جمع البيانات والمعلومات حول الجرائم الإلكترونية، يسعى المقال إلى استنتاجات عامة حول الظاهرة وتأثيراتها، مما يعكس منهجًا استقرائيًا في البحث.

2.دراسة أجنبية:

دراسة الباحثان خالد أحمد جلال، كلية الآداب، جامعة المنيا، غادة ممدوح كلية الآداب، جامعة بنها01-10-2019:

الملخص يتناول دراسة استكشافية حول العلاقة بين استخدام مواقع التواصل الاجتماعي والخوف من الوقوع ضحية للجريمة لدى الشباب، مع الأخذ في الاعتبار عوامل جودة الحياة. تم إجراء الدراسة على عينة من 1795 طالبًا في الجامعة، حيث تم استخدام استبيانات لقياس التعرض لمواقع التواصل الاجتماعي، والخوف من الجريمة، وجودة الحياة .

أظهرت النتائج أن معدل تعرض الشباب لمواقع التواصل الاجتماعي بلغ 38.4%، وأن 43% من الشباب يثقون في الأخبار المتعلقة بالجريمة التي تقدمها هذه المواقع. من بين الأسباب الرئيسية لمتابعة أخبار الجريمة، كان التعرف على مدى انتشار الجرائم وطرق الوقاية منها. كما أظهرت الدراسة أن هناك علاقة سالبة بين كثافة استخدام مواقع التواصل الاجتماعي والخوف من الوقوع ضحية للجريمة، مما يعني أن الاستخدام الكثيف لهذه المواقع قد يقلل من هذا الخوف .

بالإضافة إلى ذلك، تم تحديد الجرائم الأكثر انتشارًا بين الشباب، مثل سرقة المتعلقات الشخصية وخطف الأطفال. وأخيرًا، توصلت الدراسة إلى أن جودة الحياة تؤثر أيضًا على مستوى الخوف من الوقوع ضحية

للجريمة، حيث أن الشباب الذين يستخدمون مواقع التواصل الاجتماعي بشكل أقل كانوا أكثر عرضة للشعور بالخوف من الجرائم.

وبناء على الإشكالية نصيغ الفرضيات التالية:

فرضيات الدراسة:

- قلة ثقافة الوعي الأمني في حماية المعلومات الشخصية لدى ضحايا الجرائم الالكترونية.
- الثقة الزائدة في التعامل مع المعلومات أو الأشخاص عبر الإنترنت.

أهداف الدراسة:

- فهم الخصائص الاجتماعية والثقافية لضحايا الجرائم الالكترونية
- معرفة ثقافة استخدام الضحايا للوسائط الرقمية
- تحليل كيفية تعامل الضحايا مع الاحتيال الالكتروني

أهمية دراسة الموضوع:

أصبحت هذه الجريمة تشكل أرّق الكثير من ذوي الشأن وغيرهم؛ بل أصبحت ظاهرة بدأت بالتفشي، وأخذت طريقها في الانتشار؛ مما يتطلب ضرورة السرعة في تكوين دراسة مستفيضة لهذا العدوان الإلكتروني، وإيجاد الحلول المناسبة للتصدي لهذه الجريمة، ومحاولة تخفيف حدتها، وتقليص ضررها.

كما يستوجب تنامي هذه الجريمة أهمية توعية الآخرين بمخاطرها، وتحذيرهم من آفاتها، وإيجاد حصانة علمية وعملية تحميهم من ضررها، وتقيهم شرها، تعدد دوافع الجريمة، وتنوع أساليبها، مما أدى لتفشيها في المجتمع، وظهورها بصور وأشكال شتى.

مما سبق وأكثر يتبين أهمية هذا الموضوع، وضرورة طرحه؛ لكي نساهم ولو بشكل يسير في حماية المجتمع من المخاطر جرائم الإحتيال الإلكتروني التي تلف به، ونشارك ولو بجهد بسيط في تخليصه من المشاكل التي تحوطه.

أسباب اختيار الموضوع:

اختيار موضوع سمات ضحايا الجرائم الاحتيالية الإلكترونية يعود إلى عدة أسباب رئيسية تعكس أهمية هذا المجال في العصر الرقمي الحالي:

تزايدت الجرائم الإلكترونية بشكل ملحوظ في السنوات الأخيرة، مما يجعل من الضروري فهم العوامل التي تجعل الأفراد عرضة للاحتيال. هذا الفهم يساعد في تطوير استراتيجيات فعالة للوقاية والتوعية.

يعتمد المحتالون على استغلال جهل الضحايا بمخاطر الإنترنت، مما يستدعي ضرورة البحث في سمات هؤلاء الضحايا لفهم كيفية استهدافهم وكيفية تعزيز وعيهم بالأمان الرقمي، كما تتضمن سمات الضحايا جوانب نفسية واجتماعية تؤثر على كيفية تعرضهم للاحتيال، مثل الثقة الزائدة أو الضغوط الاقتصادية. دراسة هذه الجوانب تساعد في تقديم الدعم النفسي والاجتماعي للضحايا.

ويُعتبر هذا الموضوع مهمًا لرفع مستوى الوعي المجتمعي حول الجرائم الإلكترونية، مما يعزز من قدرة الأفراد على حماية أنفسهم وبياناتهم الشخصية. باختصار، اختيار موضوع سمات ضحايا الجرائم الاحتيالية الإلكترونية يهدف إلى فهم الظاهرة بشكل شامل، مما يسهم في تطوير استراتيجيات فعالة للوقاية والدعم.

منهج الدراسة:

تكتسي دراسة المنهج أهمية كبيرة، فمهما كان موضوع البحث، فإن قيمة النتائج تتوقف على قيمة المناهج المستخدمة، فتعرف المنهجية مجموعة المناهج والتقنيات التي توجه إعداد البحث العلمي وترتيب الطريقة

العلمية، أي هي دراسة المناهج والتقنيات المستعملة في العلوم الإنسانية والاجتماعية.

في إطار الدراسة لموضوعنا، وبناء على الإشكالية تم الاعتماد على منهج وصفي يتيح لنا توضيح الخصائص ودراسة المتغيرات، بالإضافة إلى الحصول على معلومات كافية ودقيقة..

وعليه يعتبر المنهج الوصفي الطريقة المحددة التي توصل الإنسان الباحث من نقطة إلى نقطة أخرى، أي هو عبارة عن عدد من الخطوات المنظمة التي تسهم في تنفيذ البحث بالأسلوب الصحيح.

أدوات الدراسة:

استخدام أدوات متعددة لجمع البيانات، مثل:

1. **الاستبيانات** :تصميم استبيانات تتضمن أسئلة مغلقة ومفتوحة لجمع معلومات حول السمات الشخصية والسلوكيات التقنية للضحايا.

2. **تفسير النتائج:** تفسير النتائج المستخلصة من التحليلات الكمية والنوعية، مع التركيز على العلاقة بين السمات الشخصية والظروف الاجتماعية والتعرض للاحتيال باستخدام الدراسة الميدنية

العينة:

يمكن تعريف العينة على أنها مجموعة من مجتمع الدراسة، نقوم بإجراء الدراسة عليها بالطريقة القصدية ثم استخدام النتائج لتعميمها، وقد تم اختيار عينة البحث من مستخدمي مواقع التواصل الاجتماعي (الفايسبوك) من تاريخ 2024/08/22 إلى تاريخ 2024/08/26 والتي تعتبر عينة إفتراضية من 30 فردا المتكونة من 12 ذكر و18 أنثى والمتكونة من الفئة العمرية ما بين 18-40 سنة.

صعوبات الدراسة:

تواجه عملية التواصل مع مركز الشرطة في الجزائر صعوبات كبيرة، خاصة فيما يتعلق بعدم تزويدنا بالمعلومات حول جرائم الاحتيال الإلكتروني. هذه الصعوبات تشمل:

عدم وجود قنوات اتصال فعالة: قد تكون قنوات الاتصال مع مراكز الشرطة غير واضحة أو غير متاحة بشكل كافٍ، مما يصعب الحصول على المساعدة. وعدم تجاوب الافراد للإجابة على الاستمارة الالكترونية المرسلة إليهم الا في حالات نادرة لنجمع في الأخير هذه العينة المكونة من 30 فرد فقط.

تحديد المفاهيم:

1.تعريف الجريمة:

الجريمة تُعرّف بأنها كل فعل أو امتناع عن فعل يعاقب عليه القانون، أو أنها سلوك غير مشروع ناتج عن إرادة جنائية يستوجب القانون جزاءً. تتكون المجتمعات من عدد كبير من الأفراد، ولكل فرد سماته الخاصة، حيث يوجد من يسعى للخير ومن يُظهر الشر. يُولد الإنسان بفطرة سليمة لا تعرف الإيذاء أو الإجرام، وتلعب البيئة المحيطة دورًا مهمًا في تشكيل شخصيته وتأثيرها. بعض الأفراد قد يتعرضون لتأثيرات سلبية من بيئتهم، مما يؤدي إلى انحرافهم نحو سلوكيات غير مقبولة، وبالتالي ارتكاب الجرائم. يُعزى ارتكاب الأفراد للجرائم إلى عدة أسباب، منها الانحراف الأولي، وردود فعل المجتمع، وتكرار الجرائم، ونوع الدوافع. تُقسم الجرائم بناءً على نوع الدافع إلى أربعة أنواع: جرائم سياسية، وجرائم جنسية، وجرائم اقتصادية، وجرائم اجتماعية. (قراني مفيدة، ص10)

2.تعريف الجريمة الالكترونية:

قد تباينت وجهات النظر حولها، حيث يوجد اختلاف في تحديد نطاقها وخصائصها. يمكن تعريف الجريمة الإلكترونية على أنها أي فعل غير مشروع يتم ارتكابه باستخدام التكنولوجيا الحاسوبية بمعرفة وعلم منفذ الجريمة، سواء كانت هذه الجريمة تتعلق بالتعدي على نظام معالجة البيانات، تزوير وتدمير الوثائق الإلكترونية، الاحتيال الإلكتروني، سرقة بطاقات الائتمان، القرصنة، أو غسيل الأموال.

بعض الفقهاء والباحثين يرون الجريمة الإلكترونية على أنها أي سلوك غير مشروع أو غير مسموح به يتعلق بمعالجة البيانات أو نقلها، ويتم ارتكابها بواسطة التكنولوجيا الحديثة. هذا يعني أن الجريمة الإلكترونية تشمل أي فعل غير قانوني يتم باستخدام التكنولوجيا الحاسوبية ويستهدف المصلحة العامة أو الخاصة عبر وسائل إلكترونية.

وهي نوع من الجرائم التي تتم باستخدام التكنولوجيا الحاسوبية. يمكن تعريفها على أنها أي فعل غير مشروع يتم ارتكابه باستخدام التكنولوجيا الحاسوبية بمعرفة وعلم منفذ الجريمة، سواء كانت هذه الجريمة تتعلق بالتعدي على نظام معالجة البيانات، تزوير وتدمير الوثائق الإلكترونية، الاحتيال الإلكتروني، سرقة بطاقات الائتمان، القرصنة، أو غسيل الأموال. تتضمن الجرائم الإلكترونية مجموعة متنوعة من الأنشطة غير القانونية، مثل الهجمات الإلكترونية، التي تتركز على تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر، غالباً ما يكون هدفها سياسي .وتشمل أيضاً أنواع أخرى من الجرائم مثل انتحال الشخصية، حيث يستدرج المجرم الضحية ويستخلص منها المعلومات بطرق غير مباشرة. الجرائم الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الإتصال الحديثة والشبكات المعلوماتية .وتشمل أيضاً أنواع أخرى من الجرائم مثل سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو

بيانات وحسابات خاصة بالبنوك والأشخاص.. (سيميا أبي خليل، ص6)

يجب الإشارة إلى أن الجريمة الإلكترونية لا يوجد تعريف قانوني موحد لها، وهذا يعود جزئياً إلى عدم وجود تنسيق دولي في هذا المجال وتباين التشريعات الوطنية في تحديد نطاق وتصنيف الجرائم الإلكترونية.

أولا: التعريف اللغوي:

الجريمة لغة كلمة مشتقة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقا للمفهوم الاجتماعي كل سلوك إرادي غير مشروع يصدر عن شخص مسؤول جنائيا في غير حالات الإباحة عدوانا على مال أو مصلحة أو حق محمي بجزاء جنائي.

وعرفت الجريمة أيضا: " على أنها على فعل غير مشروع صادر عن إرادة .. يقرر له القانون عقوبة أو تدبيرا احترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غير المشرع لشبكة الانترنت على المعلومة بشكل رئيسي". (هبة نبيلة هروال ،2014 ص12)

ثانيا: التعريف الاصطلاحي:

للوقوف على مفهوم الجريمة الالكترونية يقتضي منا الحال التعرض الى التعريف الفقهي لهذه الجريمة ومن ثم تبيان التعريف التشريعي.

أ- التعريف الفقهي:

بذل الفقه جهودا مضنية في محاولة لوضع تعريف محدد لماهية الجريمة

الالكترونية وانقسم الفقه بين اتجاهين الأول يضيق من مفهوم الجريمة الالكترونية والآخر يوسع من مفهومها".

ومن التعريفات التي وضعها أنصار الاتجاه المضيق أن الجريمة الالكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى، كما عرفها هذا

الاتجاه بأنها هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط، أو هي " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه. (بلقمري ناهد، 2021،ص9)

ب-التعريف التشريعي للجريمة الالكترونية:

في السابق تم تجاهل تنظيم مجال الجريمة الإلكترونية، ولكن مع تزايد الجرائم الإلكترونية وتطور التكنولوجيا، بدأت السلطات القانونية في اتخاذ إجراءات لمواجهة هذه الجرائم. تم تعديل قانون العقوبات بموجب القانون رقم 04-15 لتضمين أحكام تتعلق بالمساس بأنظمة المعالجة الآلية للبيانات، وتم تبع ذلك بقانون رقم 09-04 الذي يحتوي. قواعد خاصة للوقاية من الجرائم التقنية ومكافحتها ولذلك فالمشرع الجزائري على غرار الكثير من التشريعات لم يعرض نظام المعالجة الآلية للمعطيات وأوكل بذلك المهمة لكل من الفقه والقضاء.

ج-تعريف الجريمة الالكترونية القانون04-15

بالرجوع الى قواعد القانون 04-15 من المادة 394 مكرر 1 ثم المادة 394 مكرر نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات حيث حددها في المادة 394 مكرر بالآتي:

- الدخول وإبقاء بالغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو إبقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي:

– تصحيح أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال ألي غرض كان المعطيات المتحصل عليها من 1 إحدى الجرائم المنصوص عليها في هذا القسم.

د– تعريف الجريمة الالكترونية في حسب القانون 09–04:

حددت المادة (02) منه الجريمة الإلكترونية بقولها: يقصد في مفهوم هذا القانون بما يأتي:

الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات: تشمل المساس بأنظمة المعالجة الآلية للبيانات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو تُسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات إلكتروني.

إن الجريمة المعلوماتية تكاد تستعصي على التعريف، ذلك أن الأبحاث والدراسات التي تتعلق بها قد أوردت لها تعريفات مختلفة ومتنوعة، بحيث اتفقت جميعها على أن لا تتفق على تعريف محدد لهذه الجريمة، وتكشف النماذج المعروضة لتعريفات هذه الجريمة تعدد المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها اسم جرائم الحاسبات، أو إساءة استخدام الحاسب، أو الجرائم المرتبطة أو المتعلقة بالحاسبات، أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة أو جرائم المعلوماتية. (خالد حسن أحمد لطفي، 2019، صفحة 25)

فمن يستخدم مصطلح الجريمة المعلوماتية أراد التعبير عن الجريمة التي يكون فيها موضوع الحق المعتدى عليه المعلومة، أما من يستخدم مصطلح جرائم الانترنت فهو استخدام ضيق لأنه سيقصر هذه الجرائم على سلوكيات غير مشروعة ترتكب عن طريق الولوج إلى شبكة الانترنت دون الجرائم التي يمكن أن نتصور إمكانية ارتكابها عن طريق جهاز الكمبيوتر دون الحاجة إلى استخدام الانترنت، أما من يستخدم مصطلح

الجريمة الإلكترونية فيقصد بها الجرائم المرتكبة عن طريق الكمبيوتر وغيره من وسائل الاتصال الحديث. (المرجع السابق، صفحة 27)

تعريف الضحية:

هو الشخص أو المجموعة من الأشخاص الذين يتعرضون للإجرام أو الضرر أو الضرر النفسي أو المادي نتيجة لجريمة أو فعل إجرامي تُعرَّف الضحية بأنها ركن أساسي من أركان الجريمة التي لم تحظ بالاهتمام العلمي أو القانوني الذي يوازي الاهتمامات والدراسات التي نالها المجرم في دراسة الفعل الإجرامي حتى بداية الأربعينيات من القرن الماضي.

لقد قامت الأمم المتحدة خلال انعقاد الجمعية العامة عام 1985 بتعريف الضحايا كالآتي: قصد الأشخاص الذين أصيبوا بضرر كان فرديا أو جماعيا بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية. (أ.قدوح نور الهدى،2015،ص2)

تشمل الضحية عدة فروعات لتعريفاتها كالأتي:

من الناحية القانونية:

يُشار إلى الفرد المتأثر بشكل مباشر بالعنف على أنه "ضحية مباشرة" بموجب قانون العنف المنزلي لعام 1997. ومن ناحية أخرى، يتأثر "الضحية غير المباشرة" بالعنف على الرغم من عدم كونه المتلقي المباشر وقد يشمل ذلك الأفراد المتأثرين بالتصوير. العنف على شاشة التلفزيون أو الأطفال الذين يشهدون العنف بين والديهم. تهدف المصطلحات البديلة المستخدمة بدلاً من الضحية – مثل الناجي أو المعتدي أو المتلقي للعنف – إلى الإشارة إلى المراحل المختلفة التي قد يمر بها الأفراد المعرضون للعنف. ومع ذلك، تقترح الأدبيات المعترف بها عالميًا استخدام كلمة "الناجي" لأنها تنقل المرونة والقوة الداخلية. يحمل المصطلح

مسحة إيجابية لا تعزز الثقة بالنفس للناجية فحسب، بل تعمل أيضًا بمثابة تذكير دقيق لمقدمي الرعاية ضد التنازل الشفقة. (د.جنان الأسطة،2012،ص29)

من الناحية النفسية:

تُعرَّف الضحية بأنها الشخص الذي يتعرض للاجرام أو الضرر النفسي نتيجة لجريمة أو فعل إجرامي. تتضمن الآثار النفسية على الضحية الشعور بالضعف والفقدان للقوة والقدرة على التصرف .فقد يشعر الضحية بالذنب والخجل والاكتئاب والقلق والخوف نتيجة للجريمة التي تعرض لها. كما أن الضحية قد تعاني من اضطرابات نفسية كالاضطراب النفسي ما بعد الصدمة، والذي ينتج عن التعرض لحدث صادم كالجريمة .وقد يؤدي ذلك إلى مشاكل في النوم والتركيز والذاكرة والعلاقات الاجتماعية في بعض الحالات، قد تلوم الضحية نفسها على ما حدث لها، وتشعر بأنها تحمل جزءًا من المسؤولية عما وقع عليها .وهذا الشعور قد يؤدي إلى تدني تقدير الذات لدى الضحية. لذلك، يتطلب التعامل مع الضحايا نفسيًا توفير الدعم النفسي والاجتماعي لهم لمساعدتهم على التعافي من الآثار السلبية للجريمة. (حاج زيان وهيبة،2022، ص9)

تعريف المواقع التواصل الاجتماعي:

مواقع التواصل الاجتماعي .يعتبر مفهوم مواقع التواصل الاجتماعي من أهم المفاهيم الأكثر ارتباطا بالأنترنت وبالتالي بالواقع الافتراضي أيضا من خلال زيادة عدد مستخدميها بشكل كبير، تشمل هذه المواقع منصات مثل الفيسبوك،تويتر، سناب شات و انستجرام التي تركز على التواصل بين الأفراد والأصدقاء ومتابعة الأحداث الجارية.

تتعد وسائل التواصل الاجتماعي لدى المستخدمين وتتخصص كل منها بميزات فريدة عن الأخرى، كما أن لكل منها سلبياتها ومشاكلها .

تأتي مواقع التواصل الاجتماعي إلى الواجهة كأحد أبرز الظواهر التي أحدثت ثورة في كيفية تفاعلنا وتواصلنا في عالمنا الحديث .تُعرَّف مواقع التواصل الاجتماعي بأنها توفير أداة للقيام بعرض عدد القراءات والتحميلات لكل عضو، ومع استمرار التطور فإنها تتحول إلى مصادر مليئة بالمعلومات والأفكار والدراسات والأبحاث العلمية.

تتضمن الفوائد الرئيسية لوسائل التواصل الاجتماعي القدرة على تسهيل البحث العلمي، فتح المجال للتواصل العلمي وإنشاء العلاقات والتواصل بين الباحثين والمختصين في شتى المجالات والأماكن، مما يسهل الوصول إلى الأبحاث العلمية الجديدة من مختلف أنحاء العالم وفي أي وقت يريده الباحث. (عاصم محمد فخري،2023،ص422)

تعريف الفايسبوك:

تأسس الفايسبوك في 4 فبراير 2004 على يد مارك زوكربيرغ أثناء دراسته في جامعة هارفارد. بدأت الفكرة بإنشاء خدمة تُسمى "فيس ماتش" التي كانت تسمح للطلاب بالتصويت على جاذبية زملائهم، لكنها أُغلقت بعد فترة قصيرة بسبب انتهاكها لسياسات الخصوصية. ومن ثم، أطلق زوكربيرغ الفايسبوك كمنصة للتواصل بين طلاب هارفارد، وسرعان ما توسعت لتشمل جامعات أخرى قبل أن تصبح متاحة للجميع في عام 2006.

يقدم الفايسبوك مجموعة من الخدمات الأساسية تشمل :إنشاء الملفات الشخصية، إضافة الأصدقاء، إنضمام إلى المجموعات ومتابعة الصفحات المختلفة. (المقدادي،2013، ص34)

التفسير النظري للدراسة:

نظرية اللامعيارية:

يعتبر دوركايم أن تفسير السلوك الإجرامي يعتمد على وجود نظام معين في المجتمع. فإذا تعرض هذا النظام للخلل، يبدأ الأفراد في السعي لتحقيق رغباتهم بطرق تتعارض مع ما أقره المجتمع من نظم وقوانين. وقد يؤدي ذلك إلى زيادة معدلات الجريمة خلال فترات الأزمات الاقتصادية. حيث يربط دوركايم الظاهرة الإجرامية بالمجتمع، ويؤكد أنها ستظل قائمة طالما استمرت المجتمعات في التطور .

تعتبر الجريمة الإلكترونية تعبيرًا عن حالة مرضية معينة، حيث تشير إلى وجود خلل في النظام الاجتماعي. ويعكس هذا الخلل عدم قدرة المجتمع على تلبية بعض الرغبات والاحتياجات لأفراده، مما يدفعهم للبحث عن وسائل لتحقيقها، بما في ذلك ارتكاب الجرائم. وعندما يعجز الأفراد عن تحقيق تلك الرغبات، يلجؤون إلى جميع الوسائل المتاحة، بما في ذلك الجرائم، نتيجة غياب معيار أو قاعدة يستندون إليها في سلوكهم داخل المجتمع . (أقرور سميرة،2022)

وبالتالي، فإن الجريمة تمثل مرضًا اجتماعيًا يتطلب دائمًا طرحه للنقاش، حيث تعكس حالة المجتمع وصحته وسلامة نظامه.

تفسير نظرية الصراع في سياق الجريمة الإلكترونية:

نظرية الصراع، كما تم الإشارة إليها سابقًا، تركز على الصراعات بين الجماعات المختلفة في المجتمع وتأثيرها على السلوك الإجرامي. عند ربط هذه النظرية بالجريمة الإلكترونية، يمكننا فهم كيف تؤثر على هذا النوع من الجرائم.

في العصر الرقمي، يمكن أن تتجلى الصراعات بين الطبقات الاجتماعية من خلال الوصول غير المتكافئ إلى التكنولوجيا. الأفراد أو الجماعات من الطبقات الدنيا قد يشعرون بالإقصاء من الفرص الاقتصادية المتاحة عبر الإنترنت، مما قد يدفعهم إلى ارتكاب جرائم إلكترونية كوسيلة لتحقيق مكاسب اقتصادية أو اجتماعية، الأفراد أو الكيانات التي تمتلك السلطة في الفضاء الرقمي (مثل الشركات الكبرى أو الحكومات) قد تضع قوانين أو سياسات تحمي مصالحها، مما يؤدي إلى تهميش الأفراد الآخرين. هذا التهميش يمكن أن يؤدي إلى ردود فعل عنيفة، مثل الهجمات الإلكترونية أو القرصنة، كوسيلة للاحتجاج أو استعادة السلطة. يمكن أن تؤدي التوترات الاجتماعية والتمييز إلى سلوكيات إجرامية في الفضاء الإلكتروني. على سبيل المثال، الأفراد الذين يشعرون بأنهم مهمشون أو مضطهدون قد يلجأون إلى استخدام الإنترنت كوسيلة للتعبير عن استيائهم، مما قد يتضمن ارتكاب جرائم إلكترونية مثل التشهير أو الهجمات الإلكترونية.

التغيرات السريعة في التكنولوجيا والمجتمع، مثل العولمة، قد تؤدي إلى زيادة الصراعات. مع تزايد الاعتماد على الإنترنت، يمكن أن تتزايد الجرائم الإلكترونية كاستجابة للصراعات الاقتصادية أو الاجتماعية، حيث يسعى الأفراد إلى استغلال الفرص المتاحة عبر الإنترنت. (الأزهر و زيدان،2016، ص191)

نظرية الصراع تقدم إطارًا لفهم الجريمة الإلكترونية من خلال تسليط الضوء على كيفية تأثير على سلوك الأفراد. الجريمة الإلكترونية ليست مجرد سلوك فردي، بل هي نتيجة لصراعات أوسع في المجتمع، مما يتطلب فهمًا عميقًا للسياق الاجتماعي الذي يحدث فيه هذا النوع من الجرائم

الفصل الثاني

الجريمة الإلكترونية: نشأتها، أنواعها وتأثيراتها

تمهيد

تعتبر الجرائم الإلكترونية من الظواهر الحديثة التي نشأت بالتوازي مع تطور التكنولوجيا والإنترنت، حيث بدأت تظهر في أوائل السبعينيات مع استخدام الشبكات الإلكترونية. في البداية، كانت هذه الجرائم محدودة النطاق، لكنها تطورت بسرعة لتصبح مشكلة عالمية تؤثر على الأفراد والمؤسسات على حد سواء. تتسم الجرائم الإلكترونية بتنوعها، حيث تشمل الاختراقات، الابتزاز، والسرقة، مما يعكس طبيعة التهديدات المتزايدة في عالم متصل بشكل متزايد. ومع استمرار تطور التكنولوجيا، تبرز الحاجة الملحة لتعزيز الأمن السيبراني لحماية البيانات والمعلومات. في هذا السياق، سيتم تناول نشأة الجرائم الإلكترونية ومراحل تطورها، بدءًا من بداياتها الأولى في الستينيات وحتى التحديات الحالية التي تواجهها، مما يتيح فهمًا أعمق لهذه الظاهرة المعقدة.

نشأة ومراحل تطور الجرائم الالكترونية

1. النشأة:

نشأة الجرائم الالكترونية تعود إلى بداية استخدام الإنترنت والاتصالات الالكترونية في أوائل السبعينيات. مع التطور السريع لوسائل التكنولوجية الحديثة، ازدادت أهمية الجرائم الالكترونية كأحد أشكال الجرائم التي تتميز بها. في البداية، كانت الجرائم الالكترونية محدودة في نطاقها، لكنها سرعان ما تطورت لتصبح منتشرة في جميع أنحاء العالم.

في عام 1962، شن شخص يدعى ألين شير هجوماً إلكترونياً على شبكات الكمبيوتر في معهد ماساتشوستس للتقنية، ما يعتبر من أهم الأحداث في تاريخ الجرائم الالكترونية. منذ ذلك الوقت، ازدادت

الهجمات الإلكترونية التي تستهدف أجهزة إنترنت الأشياء، وفقاً لتقارير عدة من صناعة الأمن السيبراني الخاصة.

مع تطور الإنترنت والاتصالات الالكترونية، ازدادت أهمية الجرائم الالكترونية كأحد أشكال الجرائم التي تتميز بها. الجرائم الالكترونية تتميز بأنها يمكن أن تتم من أي مكان في العالم، دون الحاجة إلى وجود وصول فوري إلى الموقع المضطرب. هذا يسهل التخلص منها وازالتها، ما بها أكثر خطورة. (هشام بشير، 2012، الصفحات 06-07)

الجرائم الالكترونية تتنوع ما بين اختراق وتهديد وابتزاز، وسرقة، وتجسس، وغيرها من الجرائم الالكترونية التي يرتكبها المجرمين لأسباب مختلفة. بعض الأسباب الرئيسية لارتكاب الجرائم الالكترونية هي سهولة نسخها، توفر البيانات في كل مكان، طول عمر الأجهزة المستخدمة في الجريمة، وبعض الجرائم التي تتميز بها، ونشأة الجرائم الالكترونية هي نتيجة للاستخدام الخاطئ والسيئ لبعض مستخدمي الانترنت، الذين يهدفون لإلحاق الأذى بغيرهم من مستخدمي الإنترنت الآخرين. مع تطور التكنولوجيا، سيكون من الضروري أن نطور أيضاً أمن المعلومات والأمن السيبراني لمنع هذه الجرائم من التكرار. (المرجع السابق، ص06)

ثانيا: مراحل التطور:

تطورت الجرائم الإلكترونية عبر ثلاث مراحل متتابعة بموازاة مع تقدم التكنولوجيا واستخدامات الحاسوب.

في المرحلة الأولى، والتي تمتد من الستينيات إلى السبعينيات، ظهر استخدام الكمبيوتر وربطه بالشبكة، ومعها ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية. تناولت هذه المقالات موضوعات مثل التلاعب بالبيانات المخزنة، وتدمير أنظمة الكمبيوتر، والتجسس المعلوماتي، مما أثار تساؤلات حول طبيعة هذه الجرائم وما إذا كانت مجرد حالات عابرة أم ظاهرة إجرامية جديدة. تمت أبحاث تدريجياً، وفي السبعينيات

بدأ الحديث عنها كظاهرة إجرامية جديدة.

في المرحلة الثانية، بداية الثمانينيات، ظهر مفهوم جديد لجرائم الكمبيوتر والإنترنت، حيث تركزت هذه الجرائم على عمليات اختراق الأنظمة عن بعد ونشر وزرع الفيروسات الإلكترونية التي تؤدي إلى تدمير الملفات أو البرامج. أصبحت كلمة "الهاكرز" شائعة لوصف مقتحمي النظم والجناة المعلوماتيين المتفوقين.

أما المرحلة الثالثة، ففي فترة التسعينيات، شهدت الجرائم الإلكترونية تناميًا هائلًا وتغيرًا في نطاقها ومفهومها، بفعل تطور شبكة الإنترنت وسهولة الوصول إلى الأنظمة واختراق شبكة المعلومات. ظهرت أنماط جديدة وخطيرة في نفس الوقت، إذ ازدهرت الإنترنت بشكل مذهل، بعد أن كانت مجرد شبكة أكاديمية صغيرة، وتحولت إلى شبكة عالمية متشعبة. (لامية طالة،2020، ص9)

تمهيد:

الجريمة الإلكترونية هي نوع من الجرائم التي تتم باستخدام التكنولوجيا الحاسوبية والشبكات الإلكترونية. تباينت وجهات النظر حول تعريفها وتحديد نطاقها وخصائصها، إلا أنه يمكن القول بشكل عام أنها تشمل أي فعل غير مشروع يتم ارتكابه باستخدام التكنولوجيا الحديثة بقصد الإضرار بالآخرين أو تحقيق مكاسب شخصية

منظومة معلوماتية: تُعرف كنظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، حيث يقوم واحد أو أكثر من هذه الأنظمة بمعالجة البيانات تنفيذًا لبرنامج معين.

- **المعطيات المعلوماتية:** تشمل أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي تساعد في أداء وظيفة المنظومة المعلوماتية.

أنواع الجرائم الإلكترونية:

إن الجرائم الالكترونية جرائم متعددة ومتنوعة، ويصعب حصرها بسهولة، فهي تشمل أي أمر غير مشروع بدءا من عدم تسليم الخدمات أو البضائع مرورا باقتحام الكمبيوتر و التسلل إلى ملفاته، وصولا إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي كسرقة الأسرار التجارية والابتزاز عبر الانترنت، وتبيض الأموال الدولية وسرقة الهوية والقائمة مفتوحة لتشمل كل ما يمكن تصوره بما يمكن أن يرتكب عبر الانترنت من انحرافات، توجد عدة تصنيفات لجرائم الحاسب آلالي والانترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب آلالي، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكاب، وتتمثل أهم أنواعها فيما يلي:

القرصنة: هي جريمة ترتكب من اجل الوصول غير المصرح به إلى أنظمة

الكمبيوتر والشبكات لسرقة البيانات أو تخريبها. وهي تتمثل في الوصول غير المصرح به إلى أنظمة الكمبيوتر والشبكات لسرقة البيانات أو تخريبها، يشمل اعتراض البيانات بالقصد الاستفادة منها خاصة أرقام بطاقات الائتمانية، من أنشطة القرصنة تحطيم الحماية الأمنية و تطوير برمجيات خبيثة لإرسال فيروسات على شكل بريد إلكتروني. (إسراء جبريل راشد مرعي،2018،ص23)

الابتزاز الإلكتروني هو عملية تهديد وترهيب للضحية بنشر صور أو مواد فلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير قانونية .هذا النوع من

الجريمة ينتشر عبر وسائل التواصل الاجتماعي، ويستهدف فئات مختلفة من المجتمع والابتزاز الإلكتروني يشمل مجموعة من الأنشطة الخبيثة التي يقوم بها المهاجمون عبر الإنترنت بهدف ابتزاز الضحايا وتهديدهم لتحقيق أهداف شخصية أو مالية .

الأسباب الرئيسية لظهور هذه الظاهرة هي: استغلال ضعف إنسان آخر سواء كان ضعفه بشكل دائم أم مؤقت التهديد بإفشاء أمور ماسة بحياة الفرد الشخصية والخاصة جدا إخضاع الضحايا بالإكراه للامتثال لتحقيق رغبات المهاجمين. (د.سعيد زيوش،2017،ص72)

التجسس الإلكتروني: هو عبارة عن عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على معلومات غير معلنة على العلن .هذا النوع من التجسس يستهدف الأسلاك الأمنية والمعلومات السرية، وقد تطور ليشمل أدوات متطورة كأجهزة على شكل قلم أو ساعة أو ميدالية. الأقمار الصناعية تعتبر من أهم أساليب التجسس الإلكتروني، حيث تتطور هذه التقنية بشكل مستمر مع تطور التكنولوجيا .كما أن بعض أجهزة الاستخبارات تستخدم التجسس الإلكتروني للحصول على معلومات استراتيجية، مما يثير قلقًا بشأن استغلال هذه التقنيات في التنصت على المواطنين وتسريب معلوماتهم الخاصة. للحماية من التجسس الإلكتروني، يجب اتخاذ إجراءات مثل استخدام كلمات مرور قوية وعدم مشاركتها، وتفعيل إعدادات الأمان والخصوصية على حسابات وسائل التواصل الاجتماعي. (نجاري بن حاج علي فايزة،2019، ص66)

الخلاصة:

نشأة الجرائم الإلكترونية تعود إلى بداية استخدام الإنترنت والاتصالات في السبعينيات، حيث تطورت من جرائم محدودة إلى ظاهرة عالمية. في عام 1962، تم تنفيذ أول هجوم إلكتروني على معهد ماساتشوستس للتقنية، مما ساهم في زيادة الوعي حول هذه الجرائم .تتميز الجرائم الإلكترونية بأنها يمكن أن تُرتكب من

أي مكان، مما يجعلها أكثر خطورة. تشمل أنواعها الاختراق، التهديد، الابتزاز، والسرقة، وغالبًا ما ترتكب لأسباب تتعلق بالسهولة والسرعة في تنفيذها .تطورت الجرائم الإلكترونية عبر ثلاث مراحل رئيسية :

1. **المرحلة الأولى (الستينيات إلى السبعينيات)** :ظهور استخدام الكمبيوتر والشبكات، وبدء معالجة الجرائم الإلكترونية في وسائل الإعلام .
2. **المرحلة الثانية (بداية الثمانينيات)** :تركزت الجرائم على اختراق الأنظمة وزرع الفيروسات، وبرز مصطلح "الهاكرز ."
3. **المرحلة الثالثة (التسعينيات)** :شهدت الجرائم الإلكترونية نموًا هائلًا بفضل تطور الإنترنت، مما أدى إلى ظهور أنماط جديدة من الجرائم .

تتطلب مواجهة هذه الجرائم تطويرًا مستمرًا في أمن المعلومات لمواكبة التطورات التكنولوجية

تُعتبر الجريمة الإلكترونية من الظواهر المعقدة والمتطورة التي تثير قلق المجتمعات الحديثة، حيث تتنوع أشكالها وأنماطها بشكل كبير. تشمل هذه الجرائم أفعالًا غير مشروعة تُرتكب باستخدام التكنولوجيا الحاسوبية، مثل القرصنة، الاحتيال الإلكتروني، الابتزاز، والتجسس...

ومن هنا نستنتج أن الجريمة الإلكترونية تعد تحديًا مستمرًا يتطلب تعاونًا دوليًا وتنسيقًا بين السلطات القانونية والتقنية لمواجهتها بشكل فعال. يتطلب ذلك أيضًا زيادة الوعي العام حول مخاطر هذه الجرائم ووسائل الحماية الممكنة.

تتجلى أهمية مواقع التواصل الاجتماعي في تأثيرها العميق على التغيرات الاجتماعية والسياسية في المجتمعات العربية، بما في ذلك الجزائر. لقد أصبحت هذه المنصات أدوات فعالة في تشكيل الوعي الاجتماعي وتغيير العلاقات بين الأفراد، والتغير الذي يشهده اليوم يعتمد على استخدام وسائل التواصل الاجتماعي في إنتاج وتخزين وتوزيع المعلومات و، هذه الخاصية وهي عملية توفير مصادر المعلومات

لعموم الناس بشكل ميسر هي في الواقع خاصية مشتركة بين الإعلاميين القديم والجديد، الفرق هو أن الإعلام الجديد قادر على إضافة خاصية جديدة لا يوفرها الإعلام القديم وهي التفاعل وما بعد التفاعل حيث تتيح التواصل الفوري وتبادل المعلومات بشكل لم يسبق له مثيل .(مكاوي، حسن عماد وليلى حسين السيد، 2001،ص87-108)

تتضمن الإيجابيات المرتبطة بمواقع التواصل الاجتماعي توسيع دائرة العلاقات الاجتماعية، وتعزيز التفاعل بين الأفراد، مما يسهم في تشكيل رأي عام فعال. ومع ذلك، تواجه هذه المنصات تحديات عديدة، مثل مخاطر الاحتيال وانعدام الخصوصية، التي تؤثر سلبًا على الأفراد والمجتمع .في الجزائر، أدت مواقع التواصل الاجتماعي إلى ظهور علاقات اجتماعية جديدة، مع تأثيرات ملحوظة على القيم والعادات. كما ساهمت في تعزيز الوعي السياسي، على الرغم من أن التغيير الحقيقي غالبًا ما يتطلب تحولات أعمق في الذهنيات والعقليات .بشكل عام، تعكس مواقع التواصل الاجتماعي تحولًا في كيفية تفاعل الأفراد مع بعضهم البعض ومع المجتمع، مما يستدعي وعيًا أكبر حول استخدامها بشكل مسؤول لتجنب السلبيات المحتملة.

سمات ضحايا جرائم الإحتيال الالكتروني:

تمهيد:

جرائم الاحتيال عبر مواقع التواصل الاجتماعي هي موضوع يتطلب دراسة شاملة نظرًا لتزايدها وتأثيرها على الأفراد والمجتمعات. تتنوع هذه الجرائم من الاحتيال الإلكتروني إلى النصب العاطفي، مما يستدعي الوعي والتعاون بين المستخدمين والجهات الرسمية لمكافحتها .تتضمن الأنشطة الاحتيالية عبر الإنترنت استخدام أساليب متعددة مثل التصيد الاحتيالي، حيث يتم خداع الأفراد للحصول على معلومات شخصية، أو إنشاء علاقات عاطفية مزيفة لاستغلال الضحايا ماليًا. كما أن هناك أيضًا جرائم تتعلق بالتزوير والتزييف، والتي تشمل إنشاء حسابات مزيفة أو نشر معلومات غير صحيحة لتحقيق مكاسب غير مشروعة .في السياق الجزائري، يعاني الضحايا من انتهاكات متعددة لخصوصياتهم، مثل الابتزاز والتعدي على الهوية، مما يؤثر على حياتهم بشكل كبير. ومع وجود قوانين تهدف إلى حماية الضحايا، يبقى التنفيذ الفعلي لهذه القوانين وتوفير الدعم الاجتماعي من قبل المنظمات غير الحكومية أمرًا ضروريًا .أما بالنسبة للتغيرات الاجتماعية الناتجة عن ظهور مواقع التواصل الاجتماعي، فقد أدت إلى إعادة تشكيل العلاقات الاجتماعية. بينما يرى البعض أن هذه المنصات تعزز التواصل وتوسع العلاقات، يعتبر آخرون أنها تسهم في زيادة العزلة الاجتماعية .تتضمن الإيجابيات التي توفرها هذه المنصات فرصًا للتعبير عن الأفكار ودعم المستخدمين، بينما تشمل السلبيات الإدمان، التأثير السلبي على الصحة النفسية، وانعدام الخصوصية، يتطلب التعامل مع هذه الظواهر فهمًا عميقًا وإجراءات وقائية لضمان استخدام آمن وفعال لمواقع التواصل الاجتماعي.

تعريف جرائم الاحتيال عبر مواقع التواصل الاجتماعي:

الاحتيال لغة يعني الحذق وجودة النظر والقدرة على دقة التصرف فالاحتيال مطالبتك الثي بالحيل.

تعد جريمة الاحتيال الالكتروني أحد الجرائم الالكترونية والتي خلا قانون مكافحة جرائم تقنية المعلومات العماني من تعريفها ولم يكن هناك اتفاقا على تعريفها الا انه يمكن ومن هذه التعريفات تعرف الجريمة الالكترونية بأنها كل اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب.

لم يعرف المشرع العماني جريمة الاحتيال الالكتروني، ولكن الفقه عرفها بأنها

"التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات خلال عملية البرمجة أو أي وسيلة أخرى من التأثير على الحاسب الآلي حتى يقوم بعملياته بناء على هذه الأوامر أو البيانات أو التعليمات من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير للحصول على ريح عن طريق الحيلة والخداع.

كما تعرف بأنها كل فعل أو سلوك متعمد لشخص طبيعي او معنوي ويستخدم فيه التقنية الالكترونية بهدف كسب مادي غير مشروع على الأموال أو السندات وذلك عبر طرق احتيالية او اتخاذ اسم كاذب او صفة غير صحيحة. (أحمد صابرين–المعشني محمود،2023،ص5)

أنواع جرائم الاحتيال عبر مواقع التواصل الاجتماعي:

الاحتيال الإلكتروني: تشمل عمليات احتيالية عبر الإنترنت تستخدم وسائل مثل رسائل البريد الإلكتروني والرسائل الخاصة على منصات التواصل الاجتماعي لخداع الأفراد واستغلالهم مالياً.

التصيد الاحتيالي: يتمثل في إرسال رسائل مزيفة تدعو الأشخاص إلى تقديم معلومات شخصية أو مالية، مثل كلمات المرور ومعلومات بطاقات الائتمان، عن طريق التنكر بأنها من مصادر موثوقة مثل البنوك أو شركات الإنترنت المعروفة.

النصب العاطفي: يتمثل في إنشاء علاقات عاطفية مزيفة عبر مواقع التواصل الاجتماعي بهدف استغلال الضحايا مالياً عن طريق طلب الأموال أو الممتلكات تحت مسميات مختلفة.

التزوير والتزييف: يتمثل في إنشاء حسابات مزيفة أو نشر معلومات زائفة بهدف الحصول على مكاسب غير مشروعة، سواء كانت مالية أو سمعة جيدة.

الاحتيال بالإعلانات الزائفة: يتمثل في نشر إعلانات مزيفة على منصات التواصل الاجتماعي لبيع منتجات غير موجودة أو للترويج لخدمات غير حقيقية بهدف الاحتيال على الأفراد وسرقة أموالهم.

التغيرات الاجتماعية في ضل ظهور المواقع التواصل الاجتماعي:

إن من أبرز التغيرات في المجتمع الجزائري هو تغير منظومة العلاقات الاجتماعية، والذي عرف جدلية بين الباحثين، إذ تباينت الأراء بين اتجاهين، فمنهم من يرى أن هذه المواقع ساهمت في تعزيز وتقوية العلاقات بين الأفراد وتوسيعها من ناحية أخرى، بينما يرى آخرون بأن هذه المواقع هي عامل يساهم في انتشار العزلة الاجتماعية، وهذا ما نواه إليه العديد من الباحثين فيما يخص المجتمع الجزائري وخاصة في ظل انتشار هذه المواقع في الهواتف الذكية، والتي خلقت عالما خاصا لكل فرد على حدى.

يمكن التعرف على التغيرات الاجتماعية في ظل ظهور هذه الأخيرة كما يلي:

1. تأثير على السياسة والمجتمع: ظهور مواقع التواصل الاجتماعي قد أدى إلى تغيير جوهر النظريات الاتصالية وتوفير قنوات للبث المباشر، مما أثر على السياسة والتواصل الاجتماعي في المجتمع العربي.

2. تغير العلاقات الاجتماعية: ظهور منظومة علاقات اجتماعية افتراضية بديلة للعلاقات التقليدية، ونمط جديد للتواصل الاجتماعي في الأسر وتوسيع شبكة العلاقات الاجتماعية خارج المجتمع المحلي والعربي.

3. تأثيرات على القيم والمجتمعات: مواقع التواصل الاجتماعي أثرت في تغيير ملامح المجتمعات وإعطاء قيمة مضافة في الحياة السياسية، وكذلك في تحفيز الشباب على بناء علاقات جديدة وتوسيع دائرة تواصلهم. (بندر محمود نواب،2022)

من خلال هذه التغيرات الاجتماعية التي أسهمت فيها مواقع التواصل الاجتماعي تبين فيها إيجابيات وسلبيات هذه الأخيرة النى سيتم التطرق إليها:

الإيجابيات منصات التواصل الاجتماعي:

إتاحة فرص للشباب للتعبير عن أفكارهم وجمع المهتمين بها من جميع أنحاء العالم، مما يسهل انتشار الأفكار والمعلومات.

توفير الدعم والمشاركة للمستخدمين، حيث تساعد مشاركة المشاكل والخبرات على تخطي التحديات بشكل أفضل.

فتح آفاق جديدة للأفكار الرائدة والمشاريع الناشئة، من خلال استخدام التسويق الإلكتروني عبر منصات التواصل الاجتماعي.

خلق فرص عمل وظهور مسارات مهنية جديدة، مثل كتابة المحتوى التسويقي وإدارة حسابات التواصل الاجتماعي.

تمكين الاتصال الدائم بالعالم، حيث أصبح من السهل التواصل مع الأصدقاء والعائلة في أي مكان، وكذلك الحصول على المعلومات من مختلف المصادر.

توفير فرص للتسويق الذاتي والحصول على فرص عمل، من خلال منصات مهنية مثل LinkedIn التي تربط الباحثين عن عمل بأصحاب العمل، فساهمت منصات التواصل الاجتماعي في تمكين الشباب وتوسيع آفاقهم المهنية والشخصية، مع ضرورة التعامل معها بمسؤولية وحذر.

سلبيات منصات التواصل الاجتماعي:

تتضمن منصات التواصل الاجتماعي العديد من السلبيات التي تؤثر على الأفراد والمجتمعات من أبرز هذه السلبيات :

الإدمان: يمكن أن يؤدي الاستخدام المفرط لوسائل التواصل الاجتماعي إلى الإدمان، مما يؤثر سلبًا على الإنتاجية والصحة النفسية. يشعر العديد من المستخدمين بالحاجة المستمرة لتفقد حساباتهم، مما يعطل أنشطتهم اليومية .

التأثير على الصحة النفسية: قضاء وقت طويل على هذه المنصات قد يسبب مشكلات نفسية مثل الاكتئاب والقلق. كما يرتبط الاستخدام المفرط باضطرابات النوم وسوء التغذية، حيث يفضل المستخدمون البقاء متصلين بدلاً من الاهتمام بصحتهم .

اختراق الخصوصية: تساهم وسائل التواصل الاجتماعي في انعدام الخصوصية، حيث يمكن أن تتعرض المعلومات الشخصية للتسريب أو الاختراق. المستخدمون غالبًا ما يشاركون معلومات حساسة، مما يسهل الوصول إليها من قبل الآخرين .

نشر الأخبار الزائفة: تعتبر منصات التواصل الاجتماعي بيئة خصبة لنشر الأخبار الزائفة والشائعات، مما يؤدي إلى تضليل المستخدمين وزيادة الانقسامات الاجتماعية .

التأثير على العلاقات الاجتماعية: قد تؤدي هذه المنصات إلى تدهور العلاقات الشخصية، حيث يفضل البعض التواصل عبر الإنترنت بدلاً من اللقاءات المباشرة، مما يؤثر على جودة العلاقات الإنسانية .

فقدان الوقت: تعتبر وسائل التواصل الاجتماعي من أكبر مصادر إضاعة الوقت، حيث يقضي الأفراد ساعات طويلة في التصفح، مما يؤثر على التزاماتهم ومسؤولياتهم اليومية .تتطلب هذه السلبيات وعيًا أكبر من المستخدمين حول كيفية استخدام منصات التواصل الاجتماعي بشكل مسؤول لتجنب التأثيرات السلبية.

الفصل الثالث:
نتائج الدراسة الميدانية

كيفية معالجة البيانات:

تمت عملية معالجة البيانات عن طريق إنشاء استمارة ألكترونية بواسطة الحاسوب فيها أسئلة مغلوقة ومفتوحة في موقع (Google Forms) ونشرها على موقع التواصل التواصل الاجتماعي (Facebook) لعينة مستهدفة ومن خلالها تقوم عينة الدراسة بملأها أليا ووصول نتائج الدراسة إلينا تلقائيا على شكل دائرات نسبية ونسب مئوية.

تحليل المعطيات التطبيقية:

تحليل المعطيات الميدانية لدراسة جريمة الاحتيال يتطلب منهجية منظمة لجمع البيانات، وتحليلها، واستخدام النتائج للتوصل إلى استنتاجات تتعلق بأنماط الاحتيال وأن التحليل الجيد للمعطيات الميدانية يمكن أن يساهم بشكل كبير في تطوير استراتيجيات فعالة لمكافحة الاحتيال وتحسين استجابة الأنظمة القانونية والمجتمعية تجاهه.

تحليل النتائج:

أ/ خصائص مجتمع الدراسة:

الجدول رقم (1) تبين متغير السن لدى افراد العينة:

السن	التكرار	النسبة المئوية
من 18 إلى 25 عاما	25	83.34%

من 26 إلى 30 عاما	4	13.33%
من 30 إلى 40 عاما	1	3.33%
المجموع	30	100%

تحليل للجدول:

الفئة العمرية من 18 إلى 25 عامًا تشهد أعلى نسبة من حالات الاحتيال الإلكتروني، حيث تشكل 83.34% من الإجمالي. يشير هذا إلى أن الشباب في هذه الفئة العمرية هم الأكثر عرضة لهذا النوع من الاحتيال الفئة العمرية من 26 إلى 30 عامًا تمثل هذه الفئة نسبة أقل بكثير من حالات الاحتيال الإلكتروني مقارنة بالفئة السابقة 13.33%، ولكنها ما تزال ملحوظة، أما بالنسبة الفئة العمرية من 30 إلى 40 عامًا تمثل 3.33% تمثل هذه الفئة العمرية أقل نسبة من حالات الاحتيال الإلكتروني، ربما ويعود هذا الاختلاف في التوزيع بين الفئات العمرية الى اختلاف ثقافة استهلاك المواقع الاجتماعية الالكترونية بين الأجيال.

الجدول رقم (2) توزيع متغير الجنس لدى أفراد العينة:

الجنس	التكرار	النسبة المئوية
ذكر	12	40%
أنثى	18	60%
المجموع	30	100%

- **الإناث:**

- **العدد** 18 :حالة
- **النسبة المئوية**60% :

تشير البيانات إلى أن الإناث يتعرضن بشكل أكبر لحالات الاحتيال الإلكتروني، حيث يشكلن 60% من إجمالي الحالات. ربما يعود ذلك إلى استخدامات واهتمامات الإناث اتجاه منصات التواصل الاجتماعي، لهذا نجدهن أكثر عرضة للاحتيال مثل تعرضهن للاحتيال في عملية التسوق عبر الانترنت عن طريق عملية الاحتيال التي تتضمن عروضاً مغرية أو استهدافاً لمعلومات شخصية.

الذكور:

- **العدد:** 12حالة
- **النسبة المئوية:** 40%

تمثل الحالات بين الذكور 40% من إجمالي للحالات، وهو أقل نسبة من الإناث ويمكن تفسير هذا التفاوت في أنماط تفاعلهم مع هذه المواقع، إذ يكون الذكور أكثر احترازاً أو لديهم أنماط استخدام مختلفة، مثل الانخراط في أنشطة على الإنترنت قد تكون أقل تعرضاً للاحتيال، بالإضافة إلى وعيهم بالمهارات التقنية ففي أغلب الأحيان نجد مستوى الذكور أعلى من حيث الوعي بأمن المعلومات أو مهارات تقنية قد تساعدهم على تجنب بعض أساليب الاحتيال.

الجدول رقم (3) توزيع متغير الحالة المدنية:

الحالة المدنية	التكرار	النسبة المئوية
أعزب	27	90%
متزوج	3	10%
مطلق	0	0%
أرمل	0	0%
المجموع	30	100%

تشكل حالات الاحتيال الإلكتروني بين الأفراد الأعزبين نسبة 90% من الإجمالي. يشير هذا التوزيع إلى أن الأفراد غير المتزوجين هم الأكثر تعرضاً لحالات الاحتيال الإلكتروني. تمثل حالات الاحتيال الإلكتروني بين الأفراد المتزوجين نسبة 10% فقط من الإجمالي ربما بسبب المسؤوليات الأسرية وزيادة الوعي حول الأمان الرقمي.

الجدول رقم (4) توزيع متغير المستوى الدراسي:

المستوى الدراسي	التكرار	النسبة المئوية
ابتدائي	0	0%
متوسطي	0	0%
ثانوي	9	30%
جامعي	21	70%

المجموع	30	100%

تشكل حالات الاحتيال الإلكتروني بين الأفراد ذوي المستوى الدراسي الجامعي نسبة 70% من الإجمالي، مما يشير إلى أن هذه الفئة تتعرض لحالات الاحتيال بشكل أكبر مقارنة بالأفراد ذوي المستوى الدراسي الثانوي، تمثل حالات الاحتيال الإلكتروني بين الأفراد ذوي المستوى الدراسي الثانوي نسبة 30% من إجمالي الحالات. هذا يشير إلى أن الأفراد في هذه الفئة التعليمية يتعرضون لحالات الاحتيال بشكل ملحوظ.

الجدول رقم (5) توزيع متغير القيام بتعاملات التجارية:

القيام بتعاملات التجارية	التكرار	النسبة المئوية
نعم	19	63.3%
لا	11	36.7%
المجموع	30	100%

توزيع حالات الاحتيال الإلكتروني بناءً على التعاملات التجارية

1. **الأفراد الذين يقومون بتعاملات تجارية:**
   - **العدد** :19 حالة
   - **النسبة المئوية** :63.3%

يمثل الأفراد الذين يقومون بتعاملات تجارية عبر الإنترنت 63.3% من إجمالي الحالات، مما يدل على

أنهم أكثر تعرضاً للاحتيال الإلكتروني مقارنةً بالذين لا يقومون بتعاملات تجارية. يمكن تفسير هذا التوزيع بناءً على التعاملات التجارية، مثل الشراء عبر الإنترنت أو المعاملات المالية، تجذب اهتمام المحتالين لأن هذه الأنشطة غالباً ما تشمل تبادل معلومات حساسة مثل بيانات الدفع والعناوين الشخصية، وأيضا كلما زادت تعاملات الأفراد التجارية عبر الإنترنت، زادت الفرص التي قد يستخدمها المحتالون لاستهدافهم. عمليات الشراء المتكررة والتسجيل في مواقع التجارة الإلكترونية قد تعرضهم لمخاطر أكبر.

الأفراد الذين لا يقومون بتعاملات تجارية:

- **العدد** :11 حالة
- **النسبة المئوية** :36.7%

تمثل حالات الاحتيال الإلكتروني بين الأفراد الذين لا يقومون بتعاملات تجارية نسبة 36.7% من الإجمالي، وهي أقل مقارنة بالذين يقومون بتعاملات تجارية. يمكن تفسير ذلك أن الأفراد الذين لا يشاركون في التعاملات التجارية عبر الإنترنت قد يتعرضون لمخاطر أقل، حيث أنهم لا يتعاملون مع المعلومات المالية بشكل مباشر، وهؤلاء الأفراد قد يكون لديهم أنشطة رقمية أخرى، ولكن طبيعة هذه الأنشطة قد تكون أقل تعرضاً لأساليب الاحتيال الإلكتروني مقارنةً بالتعاملات التجارية.

الجدول رقم (6) توزيع متغير تقنية الدفع:

تقنية الدفع	التكرار	النسبة المئوية
نقدا	26	86.7%
إلكترونيا	4	13.3%

المجموع	30	100%

توزيع حالات الاحتيال الإلكتروني بناءً على تقنية الدفع

1. **الدفع نقداً:**
   - **العدد** :26 حالة
   - **النسبة المئوية** :86.7%

تشير البيانات إلى أن الدفع نقداً يمثل النسبة الأكبر من حالات الاحتيال الإلكتروني، حيث يشكل 86.7% من الإجمالي ويعود ذلك إلى أن الدفع نقداً غالباً ما يرتبط بمعاملات غير رقمية، مما قد يقلل من التعرض المباشر لمخاطر الاحتيال الإلكتروني المرتبطة بالتبادلات الرقمية. ومع ذلك، يمكن أن يتم الاحتيال في سياقات مختلفة مثل الاحتيال أثناء تسليم المنتجات أو الخدمات.

وقد يكون هناك تفضيل في استخدام الدفع نقداً بين الأفراد في بعض المناطق أو السياقات، مما يعكس تحفظاً تجاه المعاملات الرقمية بسبب المخاوف من الأمان الرقمي.

2. **الدفع الإلكتروني:**
   - **العدد** :4 حالات
   - **النسبة المئوية** :13.3%

يمثل الدفع الإلكتروني نسبة 13.3% من إجمالي حالات الاحتيال، وهي نسبة أقل بكثير مقارنة بالدفع نقداً لأن الدفع الإلكتروني يفتح المجال للاحتيال الإلكتروني بما في ذلك الاحتيال على بطاقات الائتمان، الاحتيال عبر البريد الإلكتروني، والهجمات الإلكترونية. ومع ذلك، فإن النسبة الأقل قد تعكس استخداماً

محدوداً لهذه الطريقة في العينة المدروسة أو وجود أنظمة أمان فعالة تقلل من حدوث الاحتيال.

ومن الممكن أن يكون الأفراد الذين يستخدمون الدفع الإلكتروني أكثر وعياً بممارسات الأمان الرقمي، مما يقلل من تعرضهم للمخاطر مقارنةً بالدفع نقداً.

الجدول رقم (7) توزيع متغير المعرفي بأنواع الاحتيال:

معرفة بأنواع الاحتيال	التكرار	النسبة المئوية
وجود معرفة	14	46.7%
عدم وجود معرفة	16	53.3%
المجموع	30	100%

توزيع المعرفة بأنواع الاحتيال الإلكتروني

1. **وجود معرفة بأنواع الاحتيال:**
   - **العدد** :14 حالة
   - **النسبة المئوية** :46.7%

تشير البيانات إلى أن 46.7% من الأفراد لديهم معرفة بأنواع الاحتيال الإلكتروني. هذه النسبة تعكس أن ما يقرب من نصف العينة المدروسة على دراية بالمخاطر المختلفة التي قد تواجهها على الإنترنت والأفراد الذين يمتلكون معرفة بأنواع الاحتيال قد يكونون أكثر وعياً بالمخاطر المحتملة، مما يمكنهم من اتخاذ خطوات وقائية لحماية أنفسهم من الاحتيال الإلكتروني وهذه المعرفة قد تكون نتيجة للتعليم أو الوعي الذي

تم تلقيه من خلال وسائل الإعلام، برامج التوعية، أو تجارب سابقة.

2. **عدم وجود معرفة بأنواع الاحتيال:**
   - **العدد** :16 حالة
   - **النسبة المئوية** :53.3%

تمثل هذه الفئة 53.3% من إجمالي العينة، وهي النسبة الأكبر، مما يدل على أن أكثر من نصف الأفراد يفتقرون إلى المعرفة بأنواع الاحتيال الإلكتروني. يمكن تفسير هذا التفاوت بسبب في نقص الوعي أو عدم الفهم بالمخاطر المحتملة مما قد يؤدي إلى تعرضهم لمخاطر أكبر في حال وقوعهم ضحايا للاحتيال الإلكتروني.

إذا كنت تعرف طرق الاحتيال الالكتروني فماهي؟ (أجوبة مفتوحة)

- احتيال عن طريق الممارسات التجارية الإلكترونية
- عدم المصداقية والكذب في النوعية
- عند الدفع الكترونيا لا يتم ارسال المنتج، او ارسال صور منتج تقوم بشرائه وعندما يصلك تجد انه مختلف تماما وليس الذي قمت بطلبه
- الاحتيال عن طريق بريدي موب
- العروض الوهمية
- انتحال الشخصية بغرض البيع (faux compte)
- عن طريق اخذ رمز السري لبطاقة الإثمان وذلك عن طريق اللعب بكلام والاستدراج وعن

طريق الدفع المسبق من اجل خدمة معينة كعمل في شركة وتكون فقط وهمية وعن طريق التحايل بمنتج معين في صورة الاعلانية منتج وعند استلام منتج اخر

- التدليس. عروض وهمية. انتحال شخصية
- طريقة الثلاثية

الجدول رقم (8) توزيع متغير التفطن في حالة الاحتيال:

التفطن في حالة الاحتيال	التكرار	النسبة المئوية
التفطن	12	40%
عدم التفطن	18	60%
المجموع	30	100%

-
- **العدد** :12 حالة
- **النسبة المئوية** :40%

تشير البيانات إلى أن 40% من الأفراد قادرون على التفطن لحالات الاحتيال الإلكتروني عند حدوثها. هذه النسبة تعكس قدرة هؤلاء الأفراد على التعرف على علامات الاحتيال واتخاذ الإجراءات المناسبة لحماية أنفسهم أي الأفراد الذين يتمكنون من التفطن لحالات الاحتيال قد يكونون أكثر وعياً بالتقنيات والأساليب المستخدمة من قبل المحتالين، وربما استفادوا من برامج توعية أو تدريب حول الأمان الرقمي.

أو وجود الخبرة السابقة في التعامل مع الاحتيال الإلكتروني قد تلعب دوراً في تحسين قدرة الأفراد على

التعرف على الحالات المشتبه بها والرد عليها بفعالية.

2. **عدم التفطن لحالة الاحتيال:**

- **العدد** :18 حالة
- **النسبة المئوية** :60%

تمثل هذه النسبة 60% من إجمالي الأفراد، مما يدل على أن أكثر من نصف العينة يفتقرون إلى القدرة على التعرف على حالات الاحتيال عند حدوثها، بعض أساليب الاحتيال قد تكون متقدمة ومعقدة لدرجة أن التعرف عليها يكون صعباً حتى للأفراد الذين لديهم بعض المعرفة بأساليب الاحتيال.

في حالة التفطن: (أجوبة مفتوحة)

- التجاهل
- الابلاغ عنها سواء الدعم الخاص بالموقع او قانونيا
- أتفادى التعامل مع الصفحة المشكوك فيها وتحذير معارفي في التعامل معهم
- عدم دفع المال قبل استلام السلعة
- حسب المادة 372من قانون العقوبات تبليغ السلطات المختصة في نوع احتيال الذي وقع اللجوء إلى القضاء ونشر وفضح الشخص الذي قام باحتيال لتوعية ووقاية

الجدول رقم (9) توزيع متغير معرفة الإجراءات القانونية اللازمة لعملية الاحتيال:

معرفة الإجراءات القانونية اللازمة لعملية الإحتيال	التكرار	النسبة المئوية
وجود معرفة	8	16.7%
عدم وجود معرفة	22	73.3%
المجموع	30	100%

توزيع المعرفة بالإجراءات القانونية لمواجهة الاحتيال الإلكتروني

1. **وجود معرفة بالإجراءات القانونية:**
   - **العدد** :8 حالات
   - **النسبة المئوية** :16.7%

تشير البيانات إلى أن 16.7% فقط من الأفراد لديهم معرفة بالإجراءات القانونية اللازمة لمواجهة الاحتيال الإلكتروني. تعكس هذه النسبة القليلة التحديات التي يواجهها الكثيرون في فهم الخطوات القانونية التي يجب اتخاذها عند مواجهة الاحتيال.

قلة الوعي بالإجراءات القانونية قد تكون نتيجة نقص في المعلومات القانونية المتاحة للجمهور حول كيفية التعامل مع حالات الاحتيال وقد تكون الإجراءات القانونية معقدة أو غير واضحة، مما يجعل الأفراد يجدون صعوبة في فهم كيفية التقدم بشكاوى أو اتخاذ إجراءات قانونية.

2. **عدم وجود معرفة بالإجراءات القانونية:**

- **العدد** :22 حالة
- **النسبة المئوية** :73.3%

تمثل هذه النسبة 73.3% من إجمالي الأفراد، مما يدل على أن معظمهم يفتقرون إلى المعرفة بالإجراءات القانونية اللازمة لمواجهة الاحتيال الإلكتروني. يمكن أن يكون نقص الوعي بالممارسات القانونية يعكس حاجة ملحة لتوفير معلومات وتدريب حول كيفية التصرف قانونياً عند التعرض للاحتيال،و وجود التحديات في الحصول على المعلومات مما يجعلون الأفراد إيجاد صعوبة في الوصول إلى المعلومات القانونية المناسبة أو قد لا يعرفون أين يطلبون المساعدة.

إذا نعم ما هذه المعلومات؟ (أجوبة مفتوحة)

- ذهاب إلى مصلحة الشرطة الإلكترونية
- القيام بشكوى مصطحبة بأدلة تثبت الاحتيال من كلام ومكان وسلعة المتفق عليها حتى المبلغ. والاجراءات القانونية الواجب على الأمن اتخاذها القبض على المحتال وتوقيف نشاطه المزيفة
- تصوير المحادثات وتسجيل المكالمات وتقديم شكوى لدى المصالح المختصة لاسترداد المال والمتابعة القضائية
- Déclaration à la police

الجدول رقم (10) توزيع متغير الثقة في السلطات الأمنية لردع الإحتيال:

الثقة في السلطات الأمنية لردع الإحتيال	التكرار	النسبة المئوية
نعم	17	56.7%
لا	13	43.3%
المجموع	30	100%

توزيع الثقة في السلطات الأمنية

1. **الثقة في السلطات الأمنية لردع الاحتيال:**
   - **العدد** 17 :حالة
   - **النسبة المئوية**56.7% :

تشير البيانات إلى أن 56.7% من الأفراد يثقون في قدرة السلطات الأمنية على ردع الاحتيال الإلكتروني. تعكس هذه النسبة أن أكثر من نصف العينة يعتقدون أن الإجراءات الأمنية والمراقبة من قبل الجهات المختصة فعّالة في مكافحة الاحتيال وقد يكون هذا التفاؤل ناتجاً عن الجهود المبذولة من قبل السلطات الأمنية والمؤسسات الحكومية لتحسين الأمان الرقمي وتعزيز الاستجابة للجرائم الإلكترونية.

ويمكن القول أن الأفراد الذين شهدوا تحسناً في مكافحة الاحتيال أو الذين تم التعامل مع قضاياهم بشكل

فعّال قد يكونون أكثر ثقة في فعالية السلطات الأمنية.

2. **عدم الثقة في السلطات الأمنية لردع الاحتيال:**

- **العدد** :13 حالة
- **النسبة المئوية** :43.3%

تمثل هذه النسبة 43.3% من إجمالي الأفراد، مما يدل على أن جزءاً كبيراً من العينة يفتقرون إلى الثقة في قدرة السلطات الأمنية على ردع الاحتيال الإلكتروني. ربما يعود ذلك إلى عدم التعامل مع قضاياهم بشكل مرضٍ أو الذين يشعرون أن السلطات لم تكن فعالة بما فيه الكفاية قد يفقدون الثقة في قدرتها على حماية الأفراد من الاحتيال.

الجدول رقم (11) توزيع متغير التحقق من مصداقية المصدر قبل التعاملات:

التحقق من مصداقية المصدر قبل التعاملات	التكرار	النسبة المئوية
القيام بالتحقق	30	100%
عدم القيام بالتحقق	0	0%
المجموع	30	100%

نتائج التحقق من مصداقية المصدر

1. **القيام بالتحقق من مصداقية المصدر:**
   - **العدد** :30 حالة
   - **النسبة المئوية** :100%

تعكس البيانات أن 100% من الأفراد يقومون بالتحقق من مصداقية المصادر قبل الشروع في التعاملات الإلكترونية. هذه النسبة المثالية تشير إلى إدراك كامل لأهمية التحقق من صحة ومصداقية المصادر في الوقاية من الاحتيال الإلكتروني.

يظهر هذا السلوك الوعي المتقدم والممارسات الجيدة لدى الأفراد في التعامل مع المعاملات الإلكترونية، مما يقلل من احتمالية الوقوع ضحية للاحتيال والتحري عن مصداقية المصدر هو إجراء وقائي أساسي يساعد في تجنب التفاعل مع مواقع أو جهات غير موثوقة، وبالتالي يقلل من مخاطر الاحتيال.

2. **عدم القيام بالتحقق:**
   - **العدد** :0 حالات
   - **النسبة المئوية** :0%

بما أن النسبة هنا هي 0%، فهذا يعني أن جميع الأفراد في العينة يدركون أهمية التحقق من المصادر ولا يتجاهلون هذه الخطوة. عدم وجود حالات عدم التحقق يعكس التزاما كاملاً بالقواعد الأساسية للحماية من الاحتيال.

في رأيك هل ترى أن النشاطات التجارية الإلكترونية أصبحت تشغل خطرا على المجتمع في ميدان الجريمة

الإلكترونية؟ (أجوبة مفتوحة)

- نعم انها مصدر يهدد المجتمع من طرف غرباء يستغلونهم
- ليست خطيرة 100% لكن هناك بعض أفراد يستغلون التهاون والجهل لبعض الأشخاص في التعاملات الإلكترونية
- يمكن القول بأن النشاطات التجارية الإلكترونية قد زادت من فرص الجريمة الإلكترونية، لكنها ليست بالضرورة "تشكل خطرًا" بحد ذاتها على المجتمع.
- زيادة فرص الجريمة الإلكترونية: مع توسع التجارة الإلكترونية، زادت فرص الاحتيال والسرقة الإلكترونية. يمكن للقراصنة استغلال الثغرات في أنظمة الأمان لاختراق البيانات الشخصية والمالية للمستخدمين.
- تطور وسائل الاحتيال: في السابق، كانت الجرائم التقليدية تتطلب التواجد المادي، أما الآن، فقد أصبحت الجرائم الإلكترونية تتطلب فقط مهارات تقنية وأجهزة متصلة بالإنترنت، مما جعل ارتكابها أسهل بالنسبة للمجرمين.
- من وجهة نظري بالعكس تسهل عمليات التجارية ولكن يجب توخي الحذر عند التعامل والتحقق من مصداقية البائع
- من جهة نعم خاصة اذا كان الدفع الكترونيا من البطاقة و لكن من جهة اخرى تسهل التعاملات التجارية اذا كانت من جهات ذات مصداقية
- نعم اصبحت تشكل خطر في ظل عدم وعي الزبون حول إجراءات وعدم مبالات حول التحايل فنسمع الكثير من تعرضوا لتحايل بمبالغ ضخمة وعدم القدرة على فعل شيء بسبب عدم أخذ الامور القانونية بعين الاعتبار .
- نعم بخصوص الاشخاص الذين لا يعرفون او كبار السن

الخاتمة

الخاتمة:

في ختام يتضح أن الجرائم الإلكترونية تمثل تحديًا معقدًا ومتزايدًا في عصر التكنولوجيا الحديثة. لقد أظهرت الدراسة أن هذه الجرائم ليست مجرد سلوكيات فردية، بل هي نتاج لصراعات اجتماعية واقتصادية أوسع، مما يتطلب فهمًا عميقًا للسياق الذي تحدث فيه .

تتطلب مواجهة هذه الظاهرة جهودًا متكاملة تشمل تعزيز الوعي العام حول مخاطر الجرائم الإلكترونية، وتطوير استراتيجيات فعالة للتصدي لها. من الضروري أن يكون الأفراد على دراية بكيفية حماية معلوماتهم الشخصية، وأن يتمتعوا بمهارات كافية للتعرف على أساليب الاحتيال المختلفة .

علاوة على ذلك، يجب على المؤسسات الحكومية والخاصة العمل معًا لتطوير سياسات أمنية قوية، وتعزيز التعاون الدولي لمكافحة هذه الجرائم التي لا تعترف بالحدود .

في النهاية، إن التصدي للجرائم الإلكترونية يتطلب التزامًا جماعيًا من جميع فئات المجتمع، من الأفراد إلى المؤسسات، لضمان بيئة رقمية آمنة ومستدامة. من خلال التعليم والتوعية، يمكننا تقليل المخاطر وتعزيز الأمن السيبراني، مما يسهم في حماية المجتمع من التهديدات المتزايدة في هذا المج

قائمة المراجع:

- قراني مفيدة، "النظرية العامة للعقوبة والجريمة" 2022/2021، جامعة الإخوة منتوري قسنطينة -1-، كلية الحقوق ص6
- سيميا أبي خليل–شادي خليل أبو عيسى، "مفهوم الجرائم المعلوماتية:إطار القانوني،طرق مواجهتها و التحديات في لبنان"، جامعة(Holy Spirit University of Kaslik) ، رقم 23، ص6
- هبة نبيلة هروال، جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2014/2013، ص ١٢٠
- بلقمري ناهد، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر مهني في الحقوق، جامعة محمد البشير إبراهيمي برج بوعريريج، كلية الحقوق، 2021/2020، ص9.
- خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية' دار الفكر الجامعي الاسكندرية، 2019، ص: 25
- (المرجع السابق، صفحة 27)
- أ.قدوح نور الهدى/أ.معتوق جمال، مساهمة الضحايا في السلوكات الاجرامية و العنيفة الواقعة عليهم في المجتم الجزائري، مجلة الاداب و العلوم الاجتماعية، كلية العلوم الاجتماعية، جامعة البليدة2،الجزائر،مجلد8 رقم 2،ص2
- د.جنان الأسطة،2012 "معجم المصطلحات و المفردات العنية على أساس النوع الاجتماعي"،

صندوق الأمم المتحدة للسكان، لبنان ص29

- أ.حاج زيان وهيبة، 2022، أعمال موجهة علم الضحايا، جامعة علي لونيس البليدة 2، الجزائر ،ص9
- عاصم محمد فخري/ ناصر محمود عبد الفتاح، استخدام الشباب الجامعي بمواقع التواصل الاجتماعي وعلاقته باتجاهاتهم نحو الشائعات، مجلة البحوث في مجالات التربية النوعية، كلية التربية النوعية، جامعة المنيا، جمهورية مصر، مجلد التاسع رقم 45، مارس2023، ص422.
- عاصم محمد فخري،2023، "استخدام الشباب الجامعي لمواقع التواصل الاجتماعي وعلاقته باتجاهاتهم نحو الشائعات"، مجلة البحوث في مجالات التربية النوعية، جامعة المنيا، مصر
- خالد غسان يوسف المقدادي،2013، "دور الشبكات الاجتماعية"، عمان، دار النفائس
- أقرورة سميرة،2022، أهم النظريات المفسرة للسلوك الإجرامي،تاريخ النشر:2022/02/12 تاريخ الإطلاع:2024/08/26 /https://www.elmizane.com
- هشام بشير، 2012، الأليات الالكترونية لمكافحة الجرائم الالكترونية، الإمارات العربية المتحدة، المركز الدولي للدراسات المستقبلية والاستراتيجية
- (المرجع السابق، ص06)
- لامية طالة/ كهينة سلام،2020، الجريمة الالكترونية: بعد جديد مفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، الجزائر، جامعة الجزائر ّ3، ص9
- إسراء جبريل راشد مرعي،2018، الجرائم الالكترونية "أهداف–أسباب–طرق الجريمة ومعالجتها، مجلة الدراسة الإعلامية – مركز الديمقراطي العربي، العدد الأول، ص23
- سعيد زيوش،2017، ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها، الجزائر، جامعة شلف، ص72

- مكاوي، حسن عماد وليلى حسين السيد (2001). الاتصال ونظرياته المعاصرة. الدار اللبنانية المصرية، الطبعة الثانية، ص87 – 108
- أحمد صابرين – المعشني محمود، 2023، المواجهة الجنائية لجريمة الاحتيال الالكتروني في التشريع العماني، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، العدد الأول، جامعة ظفار – عمان، ص5
- بندر محمود نواب– (أثر وسائل التواصل الاجتماعي على المجتمع) تاريخ النشر 2022/11/02 – تاريخ الاطلاع: 2024/08/21 https://tinyurl.com/ym489kuf

قائمة الملاحق:

- السن
- الجنس: ذكر/أنثى
- الحالة المدنية: أعزب/متزوج/مطلق/أرمل
- المستوى الدراسي: إبتدائي/متوسطي/ثانوي/جامعي
- المهنة
- هل سبق لك بالقيام بتعاملات تجارية عبر الانترنت؟ (نعم/لا)
- هل تفضل التعامل التجاري الكترونيا أم نقدا؟ (نعم/لا)
- هل لديك معرفة بأنواع الاحتيال؟ نعم/لا إذا نعم ماهي؟ (إجابات مفتوحة)
- في حالة تعرضك لعملية الإحتيال، هل يمكنك التفطن قبل وقوعها؟ (نعم/لا) إذا نعم، كيف تتعامل مع هذه الجريمة؟ (إجابات مفتوحة)
- هل لديك معلومات حول الإجراءات القانونية في حالة تعرضك للإحتيال؟ (نعم/لا) إذا نعم ما هذه المعلومات؟ (إجابات مفتوحة)
- هل تثق في السلطات الأمنية لردع الإحتيال؟ (نعم/لا)
- هل تقوم بالتحقق من مصداقة المصدر قبل التعامل التجاري؟ (نعم/لا)
- في رأيك هل ترى أن النشاطات التجارية الإلكترونية أصبحت تشغل خطراعلى الجتمع في ميدان الجريمة الإكترونية؟ (إجابات مفتوحة)