وزارة التعليم العالي والبحث العلمي

جامعة يحي فارس المدية

كلية العلوم الاجتماعية والإنسانية

قسم علم الاجتماع والديموغرافيا والفلسفة

مذكرة مقدمة لنيل شهادة الماستر في علم الاجتماع جريمة وانحراف

ضحايا النصب والاحتيال عبر مواقع التواصل الاجتماعي

دراسة ميدانية لعينة من الطلبة الجامعين بجامعة يحي فارس المدية

من إعداد الطالبتين:

*هند بن سماية .

*ياسمين لكحل.

تحت إشراف الأستاذة:

*رقية محمودي.

السنة الدراسية: 2024 م/2025 م


بسم الله الرحمن الرحيم

الإهداء :

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تحقق الطموحات،

الحمد الله على هذا الانجاز الذي طالما حلمت به ، وكان ثمرة تعب، وصبر، ودعاء لا ينقطع

إلى روح أمي الطاهرة ، التي رحلت جسدا وبقيت في قلبي دعاءا وحنينا لايزول... رحمك الله

أهدي إليك هذا التخرج عربون حب ووفاء واشتياق لاينتهي...

إلى والدي العزيز،

قدوتي وسندي من علمني معنى الإصرار والصبر، لك كل الحب والتقدير، فبفضل توجيهك أقطف اليوم ثمرة جهدي.

إلى أمي الثانية،

شكرا لأنك كنت الأم والملاذ حين ذاقت.

إلى أخواني وأخواتي،

أنتم الأمان والدعم الحقيقي ، شركاء النجاح وفرحة الانجاز،

إلى رفيق دربي ،

شكرا لأنك كنت النور حين أظلمت الأيام ، واليد التي رفعتني حين تعثرت، وجودك هو نعمة أعتز بها،

وإلى رفيقتي،

أهديك جزءا من هذا النجاح، فقد كانت لي الكلمة الطيبة والدعوة الصادقة لكم جميعا، أهدي هذا التخرج، ثمرة رحلتي وجهدي، وامتداد، حبكم ودعمكم.

هند

الإهداء :

الحمد لله الذي بنعمته تتم الصالحات، بفضل الله أهدي هذا العمل، الذي كان ثمرة سنوات من الاجتهاد والمثابرة، وكل قطرة تعب تحولت اليوم إلى فخر.....

إلى أولئك الذين كانوا النور حين أظلمت دروبي ،والسند حين أثقلتني المسؤولية ، والنبض حين خفت عزيمتي .....

إلى أمي الحبيبة، الروح التي أنجبتني مرتين: مرة إلى الحياة، ومرة إلى الأمل.

يانبع الحنان ، وصاحبة الدعاء الذي لم يخيبني يوما ، لولاك ما صبرت ولا أكملت.

دمت لي وطنا لا يغيب.

وإلى أبي العزيز، من علمني أن الرجولة ليست بالقوة، بل بالعطاء، من وقف خلفي بثبات، وسندي بصمت يشبه الجبال.

شكرا لك على إيمانك بي، وعلى كل تضحياتك التي لا تحصى.

إلى أخواتي، أنتم البهجة في قلبي، أنتم من جعلتم الطريق أقل وعورة، والرحلة أكثر دفئا.

وإلى صديقتي، رفيقة الدراسة والحياة، من تقاسمت معها التعب قبل الفرح، والقلق قبل النجاح، أهديك هذه اللحظة التي انتظرناها سويا، فلك من القلب كل الشكر والامتنان.

إلى أعز صديق دراسة على قلبي، الذي كان رفيق الدرب الطويل، من تشاركنا معا السهر والقلق، والضحك والخيبة،من كان الحضن المعنوي حين ذاقت الأيام، والصوت المشجع عندما تلعثمت خطواتي، وجودك في حياتي لم يكن صدفة، بل نعمة أحمد الله عليها كل يوم.أهديك هذا العمل لأنك لم تكن فقط صديق دراسة، بل كنت أخا ورفيقا وسندا.

أهدي هذا العمل ولكل من دعمني.....

وبفضل الله أولا، ثم بدعوات من أحب، وبدعم من أحاطوني بحبهم، تم هذا الانجاز، وأهديه اليوم لكل من كان له أثر في قلبي، ولكل من آمن أن الأحلام، حين تقترن بالإيمان والعمل، تصبح واقعا. مع دعائي أن أكون عند حسن الظن دائما...

*** الحمد لله دائما وأبدا ***

ياسمين

شكر وعرفان:

الحمد الله الذي بنعمته تتم الصالحات ، وبفضله تحققت هذه الخطوة في مسارنا العلمي ، فقد أتممنا هذا العمل المتواضع بعد جهد ومثابرة، وكان لعدد من الأشخاص الفضل الكبير في دعمنا وتشجيعنا.

نتقدم بجزيل الشكر والعرفان إلى الأستاذة المشرفة "محمودي رقية" ،التي لم تبخل علينا بعلمها وتوجيهاتها القيمة، فلها منا كل التقدير والاحترام.

ولا يسعنا إلا أن نتقدم بخالص الامتنان إلى كافة أستاذة القسم وطاقم الكلية ، على ما قدموه من علم ومعرفة طيلة سنوات الدراسة.

ولا نسى أن نوجه شكري أيضا إلى زملائي وأصدقائي الذين شاركونا لحظات التعب والفرح وكانوا سندننا وعوننا ، فلكم منا كل الحب والدعاء.

ياسمين هند

الملخص:

تهدف هذه الدراسة إلى تحليل ظاهرة ضحايا النصب والاحتيال عبر مواقع التواصل الاجتماعي من منظور سوسيولوجي ، حيث أصبحت هذه الجرائم تمثل شكلا جديدا من الانحراف الرقمي في ظل التطور التكنولوجي المتسارع، اعتمدنا على المنهج الوصفي التحليلي وتم تطبيق الدراسة ميدانيا على عينة مكونة من 76 طالب وطالبة من جامعة الدكتور يحي فارس – المدية.

وخلصنا في دراستنا إلى وجود علاقة بين قلة الوعي الأمني الرقمي وضعف التحكم التكنولوجي ، وازدياد احتمال تعرض الأفراد للنصب والاحتيال ، كما بينت النتائج أن أسلوب الحياة الرقمي ، مثل مشاركة المعلومات الشخصية ، والبحث عن العلاقات أو العروض التجارية ، يمثل عوامل محفزة للجناة لاختيار ضحاياهم.

وتوصلنا إلى ضرورة نشر ثقافة الوعي الرقمي،وتقوية آليات الحماية الاجتماعية والقانونية، إلى جانب تعزيز دور الجامعة كمؤسسة فاعلة في توعية الطلبة بمخاطر الفضاء الرقمي، للحد من انتشار هذه الظواهر الإجرامية.

Abstract:

Cette étude vise à analyser le phénomène des victimes de fraude à travers les sites de réseaux sociaux d'un point de vue sociologique, étant donné que ces crimes sont devenus une nouvelle forme de déviance numérique à la lumière du développement technologique rapide, nous nous sommes appuyés sur la méthode descriptive et analytique et l'étude a été appliquée sur le terrain à un échantillon de 76 étudiants et étudiantes de l'Université Dr Yahya Fares - Médéa.

Notre étude a conclu qu'il existe une relation entre une faible sensibilisation à la sécurité numérique et une mauvaise maîtrise technologique, et la probabilité accrue pour les individus d'être exposés à la fraude. Les résultats ont également montré que le mode de vie numérique, tel que le partage d'informations personnelles, la recherche de relations ou d'offres commerciales, représente des facteurs motivant les auteurs à choisir leurs victimes.

Nous avons conclu qu'il est nécessaire de diffuser la culture de la conscience numérique, de renforcer les mécanismes de protection sociale et juridique, et d'accroître le rôle de l'université en tant qu'institution efficace dans l'éducation des étudiants aux dangers de l'espace numérique, afin de limiter la propagation de ces phénomènes criminels.

This study aims to analyze the phenomenon of harassment and blackmail through social media from a socioiogical perspective. This crime has become a new form of digital delinquency in light of technological developments . we relied on the descripitive analytical approach and applied study to a sample consisting of 76 male and female students from Yahia Fares University-Medea.

Our study conclude that there is a relationship between digital a wareness and the ability to control technological tools , and the increased likelihood of individuals being exposed to harassment and blackmail . the results also showed that aspects of digital life , such as sharing personel information or commercial offers, represent a fertile ground for harassers to exploit this victim.

We concluded the necessity of spreading digital awareness and establishing social and legal protection nechanisms , as well as the importanse of university institutions in sensitizing student to the dangers of this crime and who to avoid falling in to such criminal traps .

الفهرس:

الإهداء: .....-
الإهداء .....-
شكر وعرفان: .....-
الملخص: .....-
فهرس الجداول:.....-
فهرس الأشكال: 11
مقدمة: ..... أ
الفصل الأول:الإطار المنهجي للدراسة. .....
تمهيد: 2
1/- أسباب اختيار الموضوع:..... 1
2/-أهداف الدراسة: 1
3/-أهمية الدراسة: 2
4/- تحديد المفاهيم: 3
5/: الإشكالية:..... 7
6/: المقاربة السوسيولوجية: 9
7/- الدراسات السابقة: 12
المبحث الثاني: الإجراءات المنهجية للدراسة 15
1/- منهج الدراسة:..... 15
2/ مجالات الدراسة:..... 16
3/ عينة الدراسة:..... 17
4/- أدوات الدراسة: 18
الفصل الثاني: الجرائم الالكترونية وعمليات النصب والاحتيال عبر مواقع التواصل الاجتماعي. 19
تمهيد..... 20
المبحث الأول: ماهية الجريمة الالكترونية. 21
1/- تعريف الجريمة الالكترونية: 21
2/- نشأة الجريمة الالكترونية:..... 22
3/- أنواع الجرائم الالكترونية: 24
4/- أنماط الجريمة الالكترونية: 26
5/- الأسباب الدافعة إلى ارتكاب الجريمة الالكترونية:..... 28
المبحث الثاني: عمليات النصب والاحتيال عبر مواقع التواصل الاجتماعي. 30
1/- ماهية النصب والاحتيال في مواقع التواصل الاجتماعي..... 30
2/-أركان جريمة النصب والاحتيال: 33
3/- العوامل المؤدية لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي: 34

4/- دور الضحية في حدوث جريمة النصب والاحتيال: 35
5/العقوبات المقررة في جريمة النصب والاحتيال في القانون الجزائري 37
6/نصائح مهمة لتجنب الوقوع في النصب والاحتيال الالكتروني: 42
7/ -إحصائيات: 44
خلاصة..... 50
الفصل الثالث: الهندسة الاجتماعية ودورها في وقوع الأفراد كضحايا للنصب والاحتيال 51
تمهيد: 51
المبحث الأول: ماهية الهندسة الاجتماعية 53
1/- مفهوم الهندسة الاجتماعية:..... 53
2/-فئات الهندسة الاجتماعية: 55
3/-أمثلة على الانتهاكات الناتجة عن الهندسة الاجتماعية:..... 57
أمثلة المحتوى المُخادِع: 57
أمثلة على الإعلانات المخادعفي ما يلي بعض الأمثلة على المحتوى المخادع في الإعلانات المضمَّنة. تظهر هذه الإعلانات كجزء من واجهة الصفحة وليس باعتبارها إعلانات. 59
4/ أنواع الهندسة الاجتماعية:..... 61
المبحث الثاني: آليات وتداعيات الهندسة الاجتماعية في الاحتيال عبر مواقع التواصل. 63
1/أسباب انتشار الهندسة الاجتماعية:..... 63
2/- مراحل الهجوم في الهندسة الاجتماعية: 64
3/- وسائل الهندسة الاجتماعية: 65
4/- النصائح التي يجب مراعاتها: 67
الخاتمة: 68
المبحث الأول : البيانات العامة..... 69
1/خصائص عينة الدراسة:..... 69
2/ عرض نتائج محور الأمن السبراني: 79
3/ عرض نتائج محور الأمن السبراني والاحتيال الالكتروني:..... 85
عرض نتائج الفرضية الأولى:..... 88
عرض نتائج الفرضية الثانية:..... 90
خاتمة: 97

فهرس الجداول:

الجدول 1: يبين نوع الجرائم المرتكبة خلال سنة 2022.....44

الجدول 2: يوضح نسبة الجرائم الالكترونية لسنة 2023: 46

الجدول 3: يوضح نسبة الجرائم الالكترونية المرتكبة سنة 2024. 48

الجدول 4: توزيع عينة الدراسة حسب الجنس 69

الجدول 5: توزيع عينة الدراسة حسب السن.....70

الجدول 6: توزيع عينة الدراسة حسب المستوى الدراسي 71

الجدول 7: توزيع عينة الدراسة حسب الإقامة 72

الجدول 8: توزيع عينة الدراسة حسب التخصص.....73

الجدول 9: اختبار (كا2) للاستقلالية لتحديد الفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للإقامة في الأحياء الجامعية 75

الجدول 10: اختبار (كا2) للاستقلالية لتحديد الفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للسن ..76

الجدول 11: اختبار (كا2) للاستقلالية لتحديد الفروق في أكثر مواقع التواصل الاجتماعي استخداما تبعا للجنس 78

الجدول 12: اختبار (كا2) للاستقلالية لتحديد الفروق في قوة كلمات المرور التي يستخدمها الطالب الجامعي حسب المستوى الدراسي 79

الجدول 13: اختبار (كا2) للاستقلالية لتحديد الفروق في معرفة أساسيات الأمن السبراني لدى الطالب الجامعي حسب المستوى الدراسي 81

الجدول 14: اختبار (كا2) للاستقلالية لتحديد الفروق في تلقي تدريب أو محاضرات عن الأمن السيبراني للطالب الجامعي حسب الإقامة 82

الجدول 15: اختبار (كا2) للاستقلالية لتحديد الفروق في تفعيل المصادقة الثنائية لدى الطالب الجامعي حسب الإقامة.84

الجدول 16: اختبار (كا2) للاستقلالية للعلاقة بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني 85

الجدول 17: اختبار (كا2) للاستقلالية للعلاقة بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني ...87

الجدول 18: اختبار (كا2) للاستقلالية لتحديد العلاقة بين معرفة أساسيات الأمن السبراني لدى الطالب الجامعي وتعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي.....88

الجدول 19: اختبار (كا2) للاستقلالية لتحديد تأثير عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي.....91

فهرس الأشكال:

الشكل1 : الصفحات التي تنخرط في ممارسات الهندسة الاجتماعي.....57

الشكل2 : نافذة منبثقة مخادعة تدّعي مساعدة المستخدم في تحديث المتصفّح.....58

الشكل 3: صفحة مزيفة لتسجيل الدخول إلى Google 59

الشكل 4: نافذة منبثقة مخادعة تدّعي أنّ أحد البرامج المثبّتة على جهاز المستخدم قديم.....60

الشكل 5: نافذة منبثقة مخادعة تدعي أنّ مصدرها مطوّر FLV 60

الشكل 6: توزيع عينة الدراسة حسب الجنس 70

الشكل 7: توزيع عينة الدراسة حسب السن.....71

الشكل 8: توزيع عينة الدراسة حسب المستوى الدراسي 72

الشكل 9: توزيع عينة الدراسة حسب الإقامة.....73

الشكل 10: توزيع عينة الدراسة حسب التخصص.....74

الشكل 11: أعمدة بيانية للفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للإقامة في الأحياء الجامعية 76

الشكل 12: أعمدة بيانية للفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للسن 78

الشكل 13: أعمدة بيانية للفروق في في أكثر مواقع التواصل الاجتماعي استخداما تبعا للجنس 79

الشكل 14: أعمدة بيانية للفروق في قوة كلمات المرور التي يستخدمها الطالب الجامعي حسب المستوى الدراسي 81

الشكل 15: أعمدة بيانية للفروق في معرفة أساسيات الأمن السبراني لدى الطالب الجامعي حسب المستوى الدراسي 82

الشكل 16: أعمدة بيانية للفروق في تلقي تدريب أو محاضرات عن الأمن السبراني للطالب الجامعي حسب الإقامة.....83

الشكل 17: أعمدة بيانية للفروق في تفعيل المصادقة الثنائية لدى الطالب الجامعي حسب الإقامة 85

الشكل 18: أعمدة بيانية للعلاقة بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني 86

الشكل 19: أعمدة بيانية للعلاقة بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني 88

الشكل20 : أعمدة بيانية لتوضيح العلاقة بين معرفية أساسيات الأمن السبراني لدى الطالب الجامعي وتعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي 90

الشكل 21: أعمدة بيانية لتوضيح تأثير عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي. 92

مقدمة

مقدمة:

أدى التطور التكنولوجي الهائل في العقود الأخيرة إلى تغير عميق في أنماط التفاعل الاجتماعي ، حيث أصبحت مواقع التواصل الاجتماعي جزءا لا يتجزء من الحياة اليومية لملايين الأفراد حول العالم، غير أن هذا الفضاء الرقمي ، الذي يبدو للوهلة الأولى وسيلة للتقارب والتواصل ، تحول في كثير من الحالات إلى مسرح لارتكاب جرائم مستحدثة ، وعلى رأسها جرائم النصب والاحتيال الالكتروني.

لقد وفرت هذه المواقع بيئة سهلة للمحتالين ، نظرا لانخفاض مستوى الرقابة وضعف الوعي الأمني لدى بعض المستخدمين ، مما جعل شريحة واسعة من الأفراد من مختلف الفئات العمرية والاجتماعية عرضة للوقوع كضحايا للاحتيال الرقمي ، سواء من خلال الرسائل المضللة ، أو الروابط المزيفة، أو العروض التجارية الكاذبة ، أو حتى ما يعرف بالعلاقات الاحتيالية.

ومع تزايد هذه الظاهرة ، بات من الضروري دراستها من منظور سوسيولوجي ، بهدف التعرف على الخصائص الاجتماعية والنفسية لهؤلاء الضحايا ، وفهم السياقات التي تؤدي إلى وقوعهم في فخاخ النصب ، خاصة في ظل غياب ثقافة الحماية الرقمية وضعف آليات الردع والوعي المجتمعي.

وعليه، تهدف هذه الدراسة إلى معالجة ظاهرة ضحايا النصب والاحتيال عبر مواقع التواصل الاجتماعي باعتبارها شكلا جديدا من الانحراف المعاصر ، مع التركيز على الجوانب الاجتماعية المؤدية إلى هذا النوع من الضحية ، في محاولة لتقديم قراءة سوسيولوجية تسهم في فهم أعمق وتحليل أشمل لهذا التهديد الرقمي المتزايد.

وقد تناولنا في دراستنا لهذا الموضوع من خلال أربعة فصول رئيسية:

- الفصل الأول : خصصناه للإطار المنهجي ، حيث تم عرض الإشكالية ، الأهداف، أهمية الدراسة ، وتحديد المفاهيم والمقاربة النظرية المعتمدة.
- الفصل الثاني: تناولنا مفهوم الجريمة الالكترونية وأنواع وأساليب الاحتيال عبر مواقع التواصل ، وأبرز العوامل المؤدية إلى ذلك.
- الفصل الثالث: ركزنا على مفهوم الهندسة الاجتماعية ودورها في تسهيل وقوع الأفراد كضحايا للاحتيال.

- الفصل الرابع:ويتضمن الجانب التطبيقي ، حيث قمنا بتحليل المعطيات الميدانية المستخلصة من عينة الدراسة وتفسيرها في ضوء الأطر النظرية.

وقد سعينا إلى تحليل رؤية سوسيولوجية تحليلية في فهم هذه الظاهرة الرقمي المتنامية ، وتدعو إلى تعزيز التوعية الرقمية وتطوير آليات الحماية للفئات المستهدفة ، خصوصا فئة الشباب الجامعي.

الفصل الأول:الإطار المنهجي للدراسة.

المبحث الأول: منهجية الدراسة.

تمهيد:

1- أسباب اختيار الموضوع .

2- أهمية الدراسة.

3- أهداف الدراسة.

4- تحديد المفاهيم.

5- الإشكالية.

6- المقاربة السوسيولوجية.

7- الدراسات السابقة.

المبحث الثاني: الإجراءات المنهجية

1- الدراسة الاستطلاعية.

2- منهج الدراسة.

3- مجالات الدراسة.

4- عينة الدراسة

تمهيد:

في ظل التقدم التكنولوجي المتسارع وانتشار وسائل التواصل الاجتماعي أصبحت هذه الأخيرة جزءا لا يتجزأ من الحياة اليومية لملايين الأفراد. ومع ما تتيحه من فرص للتواصل والتفاعل وتبادل المعلومات برزت أيضا تحديات ومخاطر متعددة ، من أبرزها جرائم النصب والاحتيال الالكتروني ، فقد استغل بعض الجناة هذه الفضاءات الافتراضية لتنفيذ مخططاتهم الإجرامية لطرق يصعب أحيانا اكتشافها أو ملاحقتها قانونيا.

إن ضحايا هذه الأفعال لا يقتصرون على فئة عمرية أو اجتماعية معينة بل تمتد أثار هذه الجرائم إلى مختلف الشرائح مما يطرح إشكاليات متعددة تتعلق بالوقاية والحماية القانونية والدعم النفسي والاجتماعي للضحايا .

وفي هذا السياق جاء هذا البحث لمحاولة فهم هذه الظاهرة من أبعادها الاجتماعية والنفسية والقانونية ، ورصد تجارب الضحايا ،وتحليل آليات الاحتيال الأكثر شيوعا ، بهدف الاهتمام في صياغة مقترحات وقائية وعلاجية أكثر فعالية .

الفصل الأول: الاطار المنهجي للدراسة

المبحث الأول: منهجية الدراسة

1/- أسباب اختيار الموضوع:

أ/- أسباب ذاتية:

1- الاهتمام الشخصي بهذا الموضوع بسبب انتشاره الواسع وتأثيره الكبير على الأفراد.

2- رغبتنا في التعرف والتعمق في الموضوع واكتشافه ، وذلك من خلال دراسته وإزالة الغموض عنه.

3- الفضول العلمي لفهم الأسباب التي يستخدمها المحتالون في خداع الضحايا عبر الانترنت.

4- تحفيز الطلبة من أجل المزيد من الدراسات المتعلقة بجريمة النصب والاحتيال عبر مواقع التواصل الاجتماعي لإيجاد الحلول لها .

ب/-أسباب موضوعية:

1/- الانتشار الواسع لعمليات النصب والاحتيال الالكتروني عبر منصات التواصل الاجتماعي وتأثيرها المتزايد على مختلف الفئات العمرية.

2/-التطور التكنولوجي الذي أدى إلى ظهور أساليب جديدة ومتطورة يصعب اكتشافها.

3/-قلة الوعي الرقمي لدى بعض المستخدمين، مما يجعلهم أكثر عرضة للاستغلال من قبل المحتالين.

4/-موضوع جديد له جوانب كثيرة جديرة بالبحث والمناقشة.

2/-أهداف الدراسة:

1/-تحليل العلاقة بين الجهل بالأمن السيبراني وزيادة الاحتيال لفهم آليات الاحتيال الالكتروني وتقديم حلول وقائية.

2/- دراسة الفئات الأكثر عرضة للاحتيال والنصب وأسباب وقوعهم ضحايا.

3/- دراسة العلاقة بين القدرة على التحكم التكنولوجي وزيادة الأفراد للنصب والاحتيال في الفضاء الرقمي .

4/- تقديم اقتراحات وإرشادات عملية لحماية المستهلكين من الوقوع ضحايا للاحتيال .

3/-أهمية الدراسة:

أ/- **أهمية علمية:**

1/- فهم أساليب المحتالين وتحليل السلوك الإجرامي الالكتروني.

2/- يدرس التأثيرات النفسية والاجتماعية على الضحايا.

3/- معرفة الأسباب الحقيقية التي تؤدي إلى وقوع الأفراد كضحايا لهذه الجرائم .

ب/- أهمية العملية :

1/- تعزيز وعي المستخدمين بكشف وتجنب عمليات الاحتيال .

2/- حمايتنا لأنفسنا والآخرين وتجنب الوقوع كضحية للنصب والاحتيال .

3/- القدرة على التمييز بين المصادر الموثوقة والمحتالين تعزز من الطهارة في التحقق من المعلومات.

4/- تحديد المفاهيم:

*** مفهوم النصب والاحتيال:**

أولا: مفهوم النصب:

أ/- لغة:

يطلق المعاصرون لفظة " النصب" على الخداع والاحتيال ، سواء كان مرتبطا بأخذ الأموال أم لا . أما في اللغة العربية، فكلمة ترتبط بالمخادعة والحيلة مثلا: نصب الفخاخ للصيد،حيث يحتال الصائد على فريسته وبالمثل ، فإن المحتال ينصب فخه بالمظاهر المزيفة والكلام المعسول ليخدع الناس، سواء كانوا بسطاء أو حتى أشخاص عاديين.

ب/- اصطلاحا:

هو الاستيلاء على مال منقول مملوك للغير وكان ذلك باستعمال طرق احتيالية من شأنها ايهام الناس بوجود مشروع كاذب ، أو إحداث الأمل للحصول على ربح وهمي أو التصرف في مال ثابت أو منقول ليس مالكه ، وإما باتخاذ اسم كاذب أوصفة غير صحيحة .[1]

ورد في القانون الجزائري: هو الاستيلاء عمد شيء مملوك ، بطرق احتيالية يقصد تملك الشيء أو على مال الغير بطريقة الحيلة نتيجة تملكه أو الاستيلاء على مال منقول للغير بناء على الإتيان بنية تملكه ، والشخص الذي يمارس النصاب أو المحتال.[2]

[1] –الشيخ عبد العزيز بن عبد الرحمان بن سعد البشرمي : جريمة النصب والاحتيال ، مكة المكرمة، مجلة العدد 391 ، رجب 1429 هجري ص 175.

[2] – عباس زكرياء: ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي، مذكرة مقدمة لنيل شهادة الماستر في علم الاجتماع جريمة وانحراف ، كلية العلوم الإنسانية والاجتماعية، جامعة جيلا لي بونعامة خميس مليانة ، 2023/2022، ص 06.

ج/- التعريف الإجرائي للنصب:

هو الاستيلاء على شيء غير مملوك باستعمال طرق احتيالية والتي تمثل في الغش والخداع والتدليس

ثانيا:مفهوم الاحتيال:

أ/- لغة:

يقال احتال من الحيلة وما أحوله من الحيلة نفسها ويقال:تحول الرجل واحتال إذا طلب الحيلة ومن أمثالهم:من كان ذا حيلة تحول.

الحول والحيل والحول والحيلة والمحالة، والاحتيال والتحول والتحيل كل ذلك: الحذق وجودة النظر والقدرة على دقة التصرف ، والحيل والحول: جمع حيلة، ورجل حول وحوله وحوالي حولول : شديد الاحتيال .

ب/- اصطلاحا:

أما الحيلة في اصطلاح الفقهاء فهي أخص من معناها في اللغة ، فهي نوع من العمل الذي يتحول به فاعله من حال إلى حال ، ثم غلب استعمالها عرفا في سلوك الطرق الخفية التي يتوصل بها إلى حصول الفرص، بحيث لايتفطن لها إلا بنوع من الذكاء والفطنة.

ت/- مفهوم الاحتيال في القانون:

أما القانونيون فيعرفون الاحتيال بأنه فعل إدعائي كاذب معزز بمظاهر خارجية يمارسها المحتال لكي يتم الاستيلاء على مال الغير .

التعريف الإجرائي للاحتيال:

هو وسيلة يستعملها المجرم من أجل الاستيلاء على مال الغير باستعمال أساليب كالخداع والكذب من أجل الحصول إلى الهدف معين كتحقيق ربح مادي.[1]

ثالثا:- تعريف جريمة النصب والاحتيال:

[1]-نفس المرجع ،الشيخ عبد العزيز بن عبد الرحمان بن سعد البشرمي، ص 178.

جاء تعريف جريمة النصب والاحتيال من خلال المادة 372 من قانون العقوبات كالتالي كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو إلى الحصول علي أي منهما أو شرع في ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خالي .[1]

التعريف الإجرائي لجريمة النصب والاحتيال:

هي استخدام وسائل احتيالية ، كالتزوير أو الخداع أو التصرف بسوء نية ،بقصد الاستيلاء على مال الغير أو الحصول على منفعة غير مشروعة.

رابعا: تعريف الضحايا:

يقصد بمصطلح "ضحايا" طبقا لإعلان المبادئ الأساسية لتوفير العدالة لضحايا وإساءة استعمال السلطة الصادرة عن الأمم المتحدة في 01 ديسمبر 1988، أولئك الأشخاص الذين أصيبوا بضرر فردي أوجما عي بما في ذلك الضرر البدني أو اللفظي أو المعاناة النفسية أو الخسارة الاقتصادية عن طريق أفعال أوحالات إهمال تشكل انتهاكا للقوانين الجنائية .[2]

كما نجد أيضا كارمن يقول: الضحية هو أي شخص يعاني من أذى أو خسارة أو صعوبات ما لأي سبب

ولقد تم استخدام مصطلح الضحايا في هذا البحث للدلالة على الأفراد الذين تعرضوا لجريمة النصب والاحتيال ثم أحذ أموالهم.[3]

التعريف الإجرائي للضحايا:

[1]– حاجي سميرة و مريش رقية: جريمة النصب والاحتيال في التشريع الجزائري ، مذكرة لنيل شهادة الماستر ، جامعة محمد بوضياف – المسيلة ، 2023/2022 ص 4.

[2]– يمينة لعبيدي: تحليل سلوك ضحايا جريمة النصب والاحتيال والعوامل المحيطة بها، مجلة الدراسات ص 323.

[3]– محمد فوزي : علم الضحايا و إسهاماته في الحقل الجنائي ، مجلة الفنون ص55.

التعريف الاجرائي للضحايا: هم الطلبة الجامعيين من عينة الدراسة الذين تعرضوا فعلسا لأحد أشكال النصب أو الاحتيال عبر مواقع التواصل الاجتماعي، كما تم الكشف عنه من خلال إجابتهم على الاستبيان، سواء تعلق ذلك بانتحال الهوية، الروابط المزيفة أو الرسائل المضللة.

5/: الإشكالية:

أصبح مصطلح الجريمة الإلكترونية أو الجريمة العابرة للحدود من أبرز وأخطر التحديات الأمنية التي تواجه العالم ضمن ما يسمى بالتقنية المعاصرة متمثلة في تكنولوجيا المعلومات والاتصالات.

فالجريمة الإلكترونية هي أي نشاط إجرامي يتم ارتكابه باستخدام الأجهزة الإلكترونية أوشيكة الانترنت، بما في ذلك : سرقة المعلومات والبيانات الخاصة، الاحتيال ، التحرش الالكتروني ، التهديد والابتزاز الالكتروني ، القرصنة واختراق أنظمة الكمبيوتر أو الشبكات ، نشر البرامج ، نشر الفيروسات أو البرامج التي تضر بالأجهزة ، انتحال هوية أشخاص آخرين لارتكاب جرائم . وتحدث الجرائم الالكترونية من خلال استغلال نقاط ضعف المستخدمين ، واستخدام مجموعة من الحيل والتقنيات لخداع الضحايا ، وسرقة معلوماتهم، أو السيطرة على أجهزتهم . [1]

ومن هذا المنطلق نجد أن الجرائم الإلكترونية تنوعت وتعددت بتنوع وتعدد مجالات الحياة ولعل أن أهم و اعقد الجرائم المتعلقة بالفضاء الرقمي ، حيث ظهرت عدة مواقع التواصل الاجتماعي لتسهيل عملية الاتصال والتواصل بين الأفراد ، ومن أشهر هذه المواقع وأكثرها استخداما هي الفيسبوك والانستغرام والتيك توك.

وفرت مواقع التواصل الاجتماعي مميزات للمستخدمين بالتواصل وتبادل المعلومات، وبالمقابل كانت مسرحا لارتكاب الجريمة وسهولتها، فقد سهلت على المجرمين للحصول على معلومات وصور شخصية ، كما سهلت الاختراق والاحتيال والتهديد والنصب على الانترنت .

يعتبر النصب والاحتيال من أهم الجرائم التي يعاقب عليها القانون الجنائي فهي جريمة يلجأ فيها الجاني إلى أساليب ووسائل احتيالية توقع المجني عليه في غلط يدفعه إلى أن يسلم ما يملكه للجاني

[1]– محمد هادي، الجرائم الالكترونية ،تهدد مستقبل أباتنا 2024 WWW.aljazeera-net.02/09 شوهد في 4 مارس 2025– على الساعة 10.52.

طواعية واختيار دون مقاومة ، وهذا يكون بسبب طمع الضحية أو أن –سذاجته جعلته فريسة سهلة أمام الجاني ،وخاصة أن النصب والاحتيال الالكتروني يصعب اكتشافه ومعاقبة الجاني عليه. [1]

وهذا ما وجب علينا نحن أهل الاختصاص تناول هذا النوع المستحدث من الجرائم وتسليط الضوء على ضحايا هاته الجرائم وإخضاعها للدراسة والتحليل

ومن هنا يمكن طرح الانشغال التالي المتضمن سؤال عام:

1) – ما هي العوامل الاجتماعية التي تجعل الأفراد عرضة للوقوع كضحايا للنصب والاحتيال عبر مواقع التواصل الاجتماعي؟

والأسئلة الفرعية:

1 – هل هناك علاقة بين مستوى جهل الأفراد بمعرفة الأمن السيبراني وزيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي

2– كيف تؤثر عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد للنصب والاحتيال في مواقع التواصل الاجتماعي

فرضيات الدراسة :

بناءا على ما تمكنا من معرفته خلال استطلاعنا حول الموضوع يمكننا تقديم تصور مبدئي عن الإجابة الممكنة على السؤالين في شكل فرضيتين:

الفرضية الأولى:

هناك علاقة بين مستوى جهل الأفراد بمعرفة الأمن السيبراني وزيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي .

[1]– عباس زكرياء ،ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي–جامعة جيلا لي بونعامة– خميس مليانة .سنة 2023/2022ص27 بتصرف.

الفرضية الثانية:

تؤثر عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد للنصب والاحتيال في مواقع التواصل الاجتماعي.

6/: المقاربة السوسيولوجية:

عند تناول أي موضوع ضمن تخصص الانحراف والجريمة، لابد من مراعاة الإشكالية التي تحيط به والالتزام بالإطار المعرفي والمنهجي الذي يحدده هذا المجال . فلا يمكن بأي حال من الأحوال تجاوز الأسس النظرية والخلفيات المعرفية التي يستند إليها التخصص، مما يفرض انسجاما في الطرح على المستويين النظري والمنهجي.

أ/- نظرية الأنشطة الروتينية:

هي واحدة من أبرز النظريات المعاصرة والتي يشار إليها بتسمية "النظريات العقلانية"

ولقد ظهرت في أواخر التسعينات لتغطية إصدارات نفسية واجتماعية بصورة عقلانية وسيتم التطرق بالتفصيل للنقاط والمبادئ الأساسية لهذه لاحقا.

التعريف بنظرية الأنشطة الروتينية ومبادئها الأساسية:

هي نظرية في علم الاجتماع وعلم الجريمة ، طورت من قبل الباحثين لورانس كوهين ومارك فيلسون عام 1979، وتعد من أهم النظريات التي تفسر أسباب حدوث الجريمة.

تنص نظرية الأنشطة الروتينية على أن الجريمة تحدث عندما تتوفر ثلاثة عناصر أساسية في الوقت والمكان نفسه،وهي:[1]

[1]- Cohenk,LE,&Felson,M.(1979).Social Change and Crime Rate Trends :A Routine Activity Approach. American Sociological Review, 44(4), 588-608. https://doi.org/10.2307/2094589.

– المتعدي ذي دافعية : وهذا ما يعني وجود مجرم لديه دوافع إجرامية (استعداد إجرامي) لارتكاب الجريمة.

– الهدف الملائم (مناسب):أي الضحية الذي تميزه مجموعة من الخصائص التي تجعل منه هدفا للمجرم.

– غياب أو فقدان الحراسة القادرة:أي أن نقص الحماية أو عدم توفرها للهدف المناسب

(للضحية) وفقا لهذه النظرية تعتبر العناصر الثلاث ضرورة لحدوث الفعل الإجرامي.كما أنه في حالة عدم توفر أي عنصر من العناصر الثلاثة لا يمكن حدوث الجريمة.

وقد أرجعت هذه النظرية ارتفاع معدلات الجريمة إلى التغير الاجتماعي الذي يحدث في المجتمعات المعاصرة وخاصة ما تعلق بالمسافة بين السكن ومكان العمل الذي من شأنه خلق فرص كبيرة لارتكاب الجرائم ، حيث انبثقت عن هذا التغير الاجتماعي أنماط جديدة من النشاط الروتيني اليومي في حياة الأفراد.

ويقصد بالروتين اليومي لحياة مجمل النشاطات اليومية التي يقوم بها الفرد في المجتمع المعاصر بشكل روتيني. دون أن يحسب لما ينتج عنها من عواقب خاصة في مجال الجريمة والوقوع ضحية لها.

ويرى أن كل من أن نظرية الأنشطة الروتينية تبحث في السياق البيئي الذي تحدث فيه الجرائم ، حيث يتقاطع مختلف الفاعلين الاجتماعيين في المكان والزمان، كما أن الأشخاص الذي تتفاعل معهم والأماكن التي تسافر غليها والأنشطة التي تشارك فيها تؤثر على احتمالية حدوث السلوك الإجرامي وتوزيعه في البيئات الاجتماعية المختلفة.[1]

تفسر حالات النصب والاحتيال عبر مواقع التواصل الاجتماعي من خلال نظرية الأنشطة الروتينية حيث تلتقي ثلاثة عوامل :وجود محتال لديه دافع (الجاني المتحفز) وضحية سهلة مثل : مستخدم يشارك معلوماته أو يثق بسهولة (الهدف المناسب) ، مع غياب وسائل الحماية مثل التحقق الأمني أو

1 –صبرينة رماش، تحليل سلوك ضحايا جريمة النصب والاحتيال والعوامل المحيطة بهم وفق نظرية الأنشطة الروتينية ، مجلة الرسالة للدراسات والسلوك والبحوث الإنسانية ، جامعة باجي مختارعنابة الجزائر،2024،ص 525.

الوعي الرقمي غياب الحراسة القادرة). استخدام الأفراد كافية يجعلهم عرضة لهذه المنصات دون احتياطات كافية يجعلهم عرضة للاستهداف من قبل المحتالين.

/- نظرية أسلوب الحياة:

رواد هذه النظرية هم كل من "هيدلنغ"و"غونفريسدون"و"غاروفالو" سنة 1978م .حيث يتساءل هؤلاء العلماء لماذا نجد شخصا أو مجموعة أكثر عرضة لأن يكون أو تكون ضحية أو ضحايا للجريمة ؟ والإجابة تكمن في العنوان أنه أسلوب حياتهم.فأسلوب الحياة والأنماط الحياتية قد تعود أناس معينون أكثر من غيرهم لأن يكونوا ضحايا أو مجنيا عليهم ، وأسلوب الحياة هذا لا يشمل الأعمال فقط ولكن أوقات الترويح أيضا وتنطلق هذه النظرية من أن الاحتمالات وقوع الفرد ضدية للجريمة مردها إلى ثلاثة عوامل رئيسية وهي:

1- أسلوب الحياة الذي يتبعه الفرد.
2- الأشخاص الذين يختلط بعضهم ببعض.
3- الأشخاص الذين يكون الفرد معرضا لهم وتم الوصول إلى هذا التصور بعد القيام الباحثين [1]

المذكورين أعلاه بدراسة مستيقظة لضحايا الجريمة من حيث نمط الجريمة (نوع الجريمة) والسن،و الأصل الجغرافي ،والخصائص الديمغرافيا الأخرى ذات العلاقة بضحايا الجريمة، حيث ظهر لباحثين أن هذه المتغيرات لها دور في حدوث الأفعال الإجرامية ، واتضح أيضا من نتائج دراسة الباحثين ، أن الأفراد يكونون معرضين للوقوع ضحايا الجريمة، تبعا لأسلوب الحياة الذي يسلكونه، وتبعا لتوعية الأفراد الذين يختلطون بهم أو يكونون معرضين لهم وهو ما يعني أن الفرد الذي يختار أسلوبا معينا في الحياة يختار أيضا (ضحايا) مع هذا الأسلوب ، درجة احتمال وقوعه ضحية للجريمة (درجة الأخطار) وهذا يعني أن الفرد نفسه له دخل في احتمالية وقوعه ضحية للجريمة تبعا لأسلوب الحياة الذي يتبعه والمكان الذي يختاره للعيش فيه،أو الأفراد الذين يختلط يبهم أو يكون عرضة لهم.[2]

[1]- جمال نسيب،لامية بوبيدي، قراءة سوسيونقدية لمضامين بعض النظريات السوسولوجية الحديثة المفسرة للجريمة:الاختيار العقلاني،أسلوب الحياة والنشاط الرتيبي نموذجا ، مجلة الدراسات وأبحاث المجلة العربية في العلوم الإنسانية والاجتماعية2022 ص173.

نظرية أسلوب الحياة تفترض أن نمط حياة الفرد وأنشطته اليومية يمكن أن يزيد من احتمال عبر مواقع التواصل نجد أن:

- الأشخاص الذين يقضون وقتا طويلا على مواقع التواصل، خاصة في التفاعل مع الغرباء، يكونون عرضة للاستهداف.
- مشاركة معلومات شخصية أو مالية بشكل علني تسهل على المحتالين اختيار الضحايا المناسبين.
- الانخراط في علاقات عاطفية أو معاملات عبر الانترنت يزيد من احتمالات وقوع في الاحتيال.

فبالتالي أسلوب الحياة الرقمي للفرد يلعب دورا كبيرا في جعله سهلا للمحتالين.

7/- الدراسات السابقة:

تعد الدراسات السابقة من أهم المصادر التي يعتمدها عليها في الأبحاث والدراسات الاجتماعية والعلمية بشكل،فهي توفر إطارا مرجعيا يساعدنا في تحديد المشكلات والظواهر التي نقوم بدراستها،مما يساعد في رسم الإطار العام لدراستنا.

لهذا السبب،لا يمكن إجراء أي بحث دون الاستناد إلى المعرفة المتراكمة التي تقدمها الدراسات السابقة ، إذ تعد بمثابة حجر الأساس الذي يبنى عليه البحث العلمي . من خلال مراجعة هذه الدراسات ، نستطيع فهم التطورات التي شهدها الموضوع قيد الدراسة ،مما يساعد في تقديم رؤية تحليلية متماسكة . وعلى الرغم من أن محاولاتنا قد تبدو بسيطة أو متواضعة ، إلا إنها تسهم في إثراء المعرفة العلمية من خلال تحليل الإشكاليات المطروحة وبناء فهم أعمق للظواهر الاجتماعية، وتسليط الضوء على التحولات الكبرى الناجمة عن التطورات التكنولوجية ، وما يترتب عليها من تأثيرات على أنماط الحياة المختلفة.

من هذا المنطلق، ينطلق البحث الاجتماعي من دراسة المعطيات الواقعية، وذلك بالاعتماد على الدراسات السابقة، وأعمال الباحثين المتخصصين في هذا المجال، سواء على المستوى المحلي أو العالمي وتساهم هذه الدراسات في توجيه البحث ضمن إطار نظري متين يفتح المجال أمام مناقشة الظواهر الاجتماعية من زوايا متعددة.

بناءا على ذلك ، تأتي هذه الدراسة لتعكس التطورات الحديثة في المجال، مع الاستفادة من نتائج البحوث السابقة،وبهذه الطريقة، يمكننا تقديم رؤية تحليلية متعمقة تسلط الضوء على الجوانب المختلفة للموضوع المدروس ، مما يثري المعرفة العلمية ويمهد لمناقشات أكثر دقة وشمولا.

أ/-دراسات جزائرية:

1/- دراسة "**عباس زكرياء**" **(2022)** بعنوان "**ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي** ،هدفت الدراسة إلى التعرف على ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي والكشف عن أهم الكيفيات التي يتم من خلالها الإيقاع بهم من قبل المحتالين والنصابين.

اعتمد على المنهج الوصفي التحليلي بالاعتماد على العينة القصدية المكونة من 08 ضحايا للنصب والاحتيال .[1]

حيث استعمل فيها الأدوات التالية : المقابلة . وقد أشارت نتائج الدراسة إلى:

- يقضي أغلب المبحوثين الذين تعرضوا إلى الأقل مرة واحدة للنصب والاحتيال معظم أوقاتهم وبشكل يومي اعتيادي بالتعاطي مع مواقع التواصل الاجتماعي كما توصل إلى أن الاستخدام المفرط لموقع التواصل الاجتماعي يعتبر سببا رئيسي ومباشر في وقوع هؤلاء الضحايا في النصب والاحتيال . كما يعتبر الطمع والإغراء والتسرع في اتخاذ القرار الصائب أحد العوامل الرئيسية لوقوعهم كضحايا.

التعقيب على الدراسة:

تعد الدراسة مهمة في تسليط الضوء على الجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي ،لكنها تحتاج إلى توسعة نطاق البحث ليشمل الجوانب القانونية والتقنية بجانب العوامل الاجتماعية والنفسية، كما أنا المنهج الوصفي التحليلي المستخدم مناسب ، لكنه بحاجة إلى تعزيز الدراسات ميدانية أكثر شمولا.

- لم توضح الدراسة مدى وعي الضحايا بالممارسات القانونية لاسترداد حقوقهم .

[1] -عباس زكرياء ، مرجع سبق ذكره .

- ركزت على عوامل نفسية مثل: الطمع والتسرع دون تحليل كافي للجوانب التقنية كضعف الأمان الرقمي .
- ينقصها توصيات واضحة حول تعزيز التوعية والحماية القانونية لمستخدمي الانترنت.

ب/- دراسة "**مهدي ربوح**"، "**زكرياء عيشي**" **(2021)**" **بعنوان العوامل المؤدية لوقوع جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي**"،هدفت الدراسة إلى معرفة أسباب جرائم النصب والاحتيال في مواقع التواصل الاجتماعي .

اعتمد فيها على المنهج التحليلي للمحتوى بالاعتماد على العينة القصدية المكونة من ضحيتين تم استعمال فيها الأدوات الآتية : استمارة تحليل المحتوى المضمون. وقد أشارت نتائج هذه الدراسة إلى:[1]

- أثبتت نتائج الدراسة أن الخصائص الفردية للضحية والمتمثلة في السن والجنس سبب من أسباب النصب والاحتيال عبر مواقع التواصل الاجتماعي.
- أثبتت نتائج الدراسة أن الخصائص الاجتماعية للضحية والمتمثلة في المهنة ونظرية أسلوب الحياة سبب من أسباب النصب والاحتيال عبر مواقع التواصل الاجتماعي.[2]

التعقيب على الدراسة:

تعالج الدراسة موضوع جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي وهو موضوع متزايد الأهمية في ظل توسع الاستخدام الرقمي.

تعتمد الدراسة على تحليل العوامل المؤدية لهذه الجرائم، لكن من الضروري تقييم دقة منهجيتها ومدى شمولية النتائج، كما يطرح تساؤل حول فعالية الحلول المقترحة للحد من هذه الظاهرة .ورغم أهمية الدراسة في تسليط الضوء على المشكلة، يبقى تقييمها مرتبطا بمدى دقة التحليل وملائمة التوصيات المقدمة.

[1]- مهدي ربوح ، زكرياء العيشي ، العوامل المؤدية لوقوع جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي الفايسبوك نموذجا،مذكرة مكملة لنيل ما ستر في تخصص علم الاجتماع الانحراف والجريمة ،كلية العلوم الاجتماعية والإنسانية ، جامعة الكلي محمد أو لحاح بالبويرة ، سنة 2021-2022 .

المبحث الثاني: الإجراءات المنهجية للدراسة

1/- منهج الدراسة:

أ/- المنهج:

يقصد بالمنهج الطريقة التي يتبعها الباحث في دراسة موضوع ما.

هو مجموعة من القواعد العامة التي يعتمدها الباحث في تنظيم ما لديه من أفكارأومعلومات من اجل توصله إلى النتيجة المطلوبة .

إن اختيار منهج البحث في دراسته أي موضوع لا يأتي نتيجة اختيار عشوائي ، أو بمجرد

ميل الباحث لمنهج معين دون مناهج أخرى ، فهي قضية تفرضها طبيعة البحث أو المشكلة التي يتناولها الباحث للمنهج لأنه يحدد للباحث المسار الذي يسلكه للوصول إلى نتائج علمية وموضوعية حول موضوع دراسته.[1]

وفي هذا الدراسة اعتمدنا على المنهج الوصفي التحليلي الذي يصف الظاهرة التي بصدد دراستها وهي: " ضحايا النصب والاحتيال عبر مواقع التواصل الاجتماعي".

ب/- المنهج الوصفي التحليلي:

يعرف بأنه احد المناهج الأساسية في البحث العلمي، ويعتمد على دراسة الظواهر كما هي موجودة في الواقع ، حيث يبدأ بوصفها وصفا دقيقا ، ثم ينتقل إلى تحليل مكوناتها وعلاقتها ، بغرض تفسيرها والوصول إلى استنتاجات علمية دقيقة ، فهو لا يقتصر على الوصفي فقط بل يمد إلى تفسير البيانات وتصنيفهم واستخلاص المؤشرات الدالة.[2]

---

[1]- محمد سرحان علي المحمودي: مناهج البحث العلمي ، الجمهورية اليمنية صنعاء ، ط 3 ، دار الكتب 2019 ص 35.

[2]-ملحم سامي محمد : مناهج البحث العلمي في العلوم التربوية والنفسية ، عمان الأردن ، ط 3 دار النشر المسيرة للنشر والتوزيع ، ص 200.

كما يوضح أن المنهج الوصفي التحليلي يمزج بين الوصف الكمي للظاهرة وتحليل مضامينها بهدف الكشف عن العوامل المؤثرة فيها والتوصل إلى نتائج يمكن تعميمها .[1]

كما يتيح للباحث تحليل الظاهرة بعد جمع المعلومات الدقيقة حولها، مما يساعد على تفسير الظواهر الاجتماعية والإنسانية بموضوعية.[2]

يقوم هذا المنهج على وصف ظاهرة من الظواهر ، للوصول إلى أسباب هذه الظاهرة ، والعوامل التي تتحكم فيها، واستخلاص النتائج لتعميمها ، ويتم ذلك وفق خطة بحثية معينة وذلك من خلال تجميع البيانات ، وتنظيمها ، وتحليلها.[3]

2/ مجالات الدراسة:

أ/- المجال المكاني: أجريت هذه الدراسة على عينة من الطلاب الجامعيين بجامعة يحي فارس المدية.

ب/- المجال الزمني: من 25فيفري إلى 15 جوان 2025.

[1]- أحمد مصطفى محمد : مناهج البحث العلمي بين النظرية والتطبيق ، القاهرة ، مصر ط 2، دار الوفاء لدنيا الطباعة والنشر ، 2008 ص 189- 190.

[2]- عقل حسن حسين : مناهج البحث العلمي ، الأسس والتطبيقات ، بيروت لبنان ، ط1 ، دار الفكر العربي 2006 ص 255 -256 .

[3]-محمد الصاوي محمد مبارك : البحث العلمي أسسه وطريقة كتابته ، القاهرة ،مؤسسة الإسراء للنشر والتوزيع ط1،ص 30.

3/ عينة الدراسة:

تعرف العينة على أنها جزء من المجتمع يتم اختيارها وفق قواعد خاصة بحيث تكون العينة المصحوبة ممثلة قدر الإمكان لمجتمع الدراسة.[1]

لذلك يمكن تعريف العينة على أنها مجموعة من الوحدات التي يتم اختيارها من المجتمع الإحصائي ويجب أن تكون تمثيلا صادقا ومتكافئا مع المجتمع الأصلي .[2]

تم اختيار العينة القصدية من مجتمع الدراسة تتكون من (76 طالب وطالبة) ومن تتوفر فيهم شروط استخدام شبكات التواصل الاجتماعي بشكل منتظم ،ومن تعرضوا للنصب والاحتيال وتم توزيع العينة بحسب متغيرات الجنس والسن ، والمستوى الجامعي ، بغرض تمثيل أدق لواقع ضحايا النصب والاحتيال في الفضاء الرقمي ، وقد تم جمعنا البيانات باستخدام الاستبيان.

العينة القصدية:

هي العينة التي يختارها الباحث بشكل متعمد، وفقا لخصائص معينة يرى أنها تمثل أفراد المجتمع محل الدراسة ، وذلك لأنهم الأنسب للإجابة على أسئلة البحث.[3]

---

[1]– محمد عبد العال النعيمي وآخرون: طرق ومناهج البحث العلمي ،عمان، الوراق للنشر والتوزيع ،2015 ص 78.

[2]– يوسف عبد الأمير طباجة : منهجية البحث تقنيات ومناهج ، بيروت ، دار الهادي للطباعة والنشر والتوزيع 2007 ص 160.

[3]– عبد الرحمان عدس :مناهج البحث العلمي ، دار المسيرة للنشر والتوزيع 2004،ص153.

4/- أدوات الدراسة:

- **الاستبيان:**

يعتبر الاستبيان تقنية أساسية في جمع المعلومات التي يتطلبها البحث الميداني ،وبناء على طبيعة الموضوع فإنه يفرض علينا نوع الأدوات المناسبة لذلك .لهذا اعتمدنا على أداة الاستمارة التي تعرف بأنها أداة من أدوات البحث العلمي ، معدة لجمع البيانات بهدف الحصول على إجابات مجموعة من الأسئلة والاستفسارات المكتوبة في نموذج اعد لهذا الغرض ويقوم المبحوثين بتسجيل إجابتهم بأنفسهم

أو هي أداة تتكون من مجموعة من الأسئلة توجه أو ترسل أو تسلم إلى الأشخاص الذين يتم اختيارهم لموضوع الدراسة ، ليقوموا بتسجيل إجابتهم على الأسئلة الواردة بعد ذلك للباحث.[1]

ولقد تمت الاستعانة بتقنية الاستمارة التي تيسر لنا من خلالها الكشف عن أسباب وقوع الأفراد كضحايا للنصب والاحتيال.

5/- صعوبات الدراسة:

- عدم تمكننا من اجراء دراسة حالة مباشرة لضحايا النصب والاحتيال عبر مواقع التواصل الاجتماعي وذلك بسبب غياب التنسيق الرسمي بين الجامعة والهيئات المعنية كجهاز الشرطة والمحكمة القضائية ، حيث لم يكن هناك اتفاق أو بروتوكول تعاون يسمح لنا بالوصول إلى المعطيات أو الحالات الواقعية.وقد حال هذا العائق دون جمع بيانات نوعية متعمقة من مصادرها الاصلية مما اضطررنا إلى تعديل توجه الدراسة نحو اجراء بحث ميداني على عينة من الطلبة الجامعيين بجامعة المدية يحي فارس .

[1]- رشيد زرواتي : تدريبات على منهجية البحث العلمي في العلوم الاجتماعية ، الجزائر ، ديوان المطبوعات الجامعية 2008 ص 182.

<u>الفصل الثاني</u>: الجرائم الالكترونية وعملياتالنصب والاحتيال عبر مواقع التواصل الاجتماعي.

تمهيد

المبحث الأول: ماهية الجرائم الالكترونية.

1- تعريف الجريمة الالكترونية.

2- نشأة الجريمة الالكترونية.

3- أنواع الجرائم الالكترونية.

4- أنماط الجريمة الالكترونية.

5- دوافع ارتكاب الجريمة الالكترونية.

المبحث الثاني:عمليات النصب والاحتيال عبر مواقع التواصل الاجتماعي

1- تعريف النصب والاحتيال في الانترنيت.

2- أشكال النصب والاحتيال.

3- العوامل المؤدية للنصب والاحتيال عبر مواقع التواصل الاجتماعي.

4- دور الضحية في حدوث جريمة النصب والاحتيال.

تمهيد:

مع الانتشار الواسع لاستخدام الانترنيت ومواقع التواصل الاجتماعي، ظهرت أنماط جديدة من الجرائم يطلق عليها الجرائم الالكترونية، ومن أبرزها جرائم النصب والاحتيال، يستغل الجناة هذه المنصات للإيقاع بالضحايا من خلال أساليب مخادعة مثل انتحال الهوية، الروابط الوهمية أو الوعود الكاذبة، وتشكل هذه الجرائم تهديدا حقيقيا للفرد والمجتمع، مما يستدعي دراستها وفهم أسبابها وسبل الوقاية منها.

المبحث الأول: ماهية الجريمة الالكترونية.

1/- تعريف الجريمة الالكترونية:

تتكون الجريمة الالكترونية(**Cyber Crime**) من مقطعين هما الجريمة(crime) والالكترونية (cyber)، يستخدم مصطلح الالكترونية لوصف عصر المعلومات ، أما الجريمة هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصال مثل: الانترنت مثل: غرف الدردشة والبريد الالكتروني والموبايل.[1]

وتعرف بأنها أي مخالفة ترتكب من أفراد أوجما عات بدافع جرمي ونية الإساءة لسمعة الضحية ولجسدها ،سواء كان بطريقة مباشرة وغير مباشرة أو يتم ذلك باستخدام وسائل الاتصالات الحديثة ،أي أنها كل سلوك غير قانوني ،يتم باستخدام الأجهزة الالكترونية. [2]

وقد عرفها فقهاء القانون": **بأنها كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ،ورغم أنه وقع اختلاف في تسميتهما ،إلا أن المصطلحات الأكثر شيوعا هي :جرائم الكمبيوتر ،الجرائم الالكترونية ،الجرائم المعلوماتية ، وظاهرة الغش المعلوماتي والاختلاس المعلوماتي**".

حيث يفضل جانب من الفقهاء أن يطلقوا عليها اصطلاح "جرائم التكنولوجيا الحديثة" أما الرأي الغالب والذي يميل إليه هو استعمال مصطلح "الجريمة المعلوماتية " أو الجريمة الالكترونية عام ويشمل التقنية الحالية والمستقبلية.[3]

[1]- جريمة الابتزاز الالكتروني ،دراسة ميدانية علمية .طلبة جامعة المدية . العلوم القانونية والاجتماعية.

[2]- سواكري الطاهر ، نمطية الجريمة في المجتمع الجزائري ، مخبر الجريمة والانحراف بين الثقافة والتماثلات الاجتماعية .ط1. 2022 .ص 278.

[3]- نفس المرجع .ص 279.

التعريف القانوني للجريمة الالكترونية:

فقد اصطلح المشرع الجزائري على تسميتها بمصطلح **الجرائم المتصلةبتكنولوجيا الإعلام والاتصال** ، وقد عرفها بموجب أحكام المادة 02 من القانون رقم 09-04 على أنها: "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات ،وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية ، أو نظام الاتصالات الالكترونية**".

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار ذو النظام لمعلوماتي لتحديد معالم الجريمة ، فسمى الجرائم الموجهة ضد النظام لمعلوماتي بجرائم المساس بأنظمة المعالجة ، الآلية للمعطيات ،كما بينها في قانون العقوبات من المادة394 مكرر إلى 394مكرر07 ، وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية ونظام للاتصالات الالكترونية.

ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر ، تسرب أسئلة البكالوريا2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطات الفيدرالية الأمريكية.[1]

2/- نشأة الجريمة الالكترونية:

إن مفهوم الجريمة الالكترونية مر بتطور تاريخي تبعا لتطور التقنيات واستحداثها وخاصة بعد أن أصبحت المجتمعات تعتمد على الحاسب الآلي بشكل رئيسي.

لقد مرت الجريمة الالكترونية في تطورها بعدة مراحل منذ رصدها في الإحصائيات لأولمرة في الفترة (1971-1990) تضمنت أبرز الجرائم التي رصدها وضبطها على نطاق العالم وهي قليلة جدا ويتراوح عددها بين جريمة واحدة إلى ثلاثة في العالم وأشهرها في عام 1988م عندما استخدم الحاسب الآلي لسرقة 70 مليون دولار من بنك شيكاغو الوطني الأول ، وفي ذات العام 1988م لأول مرة تكوين فريق طوارئ الحاسب الآلي (**CERT**) في معهد هندسة البرمجيات بجامعة "**كارنيجي ميلون**" الأمريكية

[1]-- الطالبة نايري عائشة ،الجريمة الالكترونية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر في القانون الاداري، كلية الحقوق والعلوم السياسية ، جامعة أحمد درية – أدرار. 2016-2017 .ص 09 .

لمواجهة الجريمة الالكترونية بأشكالها المختلفة . وفي عام 1989 تبنت اللجنة الوزارية لمجلس أوروبا التوصية رقم 9(89) الخاصة بمواجهة جرائم الحاسب الآلي.

وفي عقد التسعينات ارتفع معدل الجرائم الالكترونية نسبيا وكان أشهرها عام 1994م عندما كان عدد مستخدمي الانترنت حول العالم 25.454.590 مليار اخترق طالب أمريكي عمره 16 سنة اسم الشهرة **data stream**(نهر البيانات) أجهزة الكمبيوتر في معهد أبحاث الطاقة كوري- وكالة ناسا ووكلات حكومية أمريكية أخرى وتم اعتقاله في انجلترا. وفي عام 1995 تمكنت عصابة روسيا محترفة من سرقة عشرة ملايين دولار من مصرف **سيتي بنك** باستخدام الكمبيوتر وتحويلها إلى حسابات في فلندا وإسرائيل .وبدأت العملية الإجرامية الالكترونية في التزايد في مختلف دول العالم إلى يومنا هذا وبدأت الجهود الدولية والإقليمية بوضع استراتيجيات للوقوف في وجه هذه الجرائم المستحدثة. [1]

مرت الجرائم الالكترونية بتطور تاريخي تبعا لتطور تقنية واستخداماتها، ولهذا يمكننا القول بأن تلك الجرائم مرت بثلاث مراحل يمكن إيجازها على النحو التالي:

المرحلة الأولى: تتمثل في شيوع استخدام الحواسيب في الستينات والسبعينات،ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر، وعالجت عددا من قضايا الجرائم الفعلية ، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لامجرد سلوكيات مرفوضة.

المرحلة الثانية:في الثمانيات طفا على السطح مفهوم جديد للجرائم الالكترونية ارتبط بعمليات اقتحام نظام الكمبيوتر عن بعد، وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات والبرامج.
المرحلة الثالثة: وتتمثل في فترة التسعينات حيث شهدت تناميا هائلا في حفل الجرائم الالكترونية، وتغييرا

[1]- عفاف بعون، نسيمة أولاد سالم، الجريمة الالكترونية –قراءة سوسيو تاريخية في النشأة والآثار، مجلة القبس للدراسات النفسية والاجتماعية /المجلد (05) العدد (20) 2023 ص(من 72 إلى 74).

في نطاقها ومفهومها،وكان بفعل ما أحدثته شبكة الانترنت من تسهيل لعملية دخول الأنظمة واقتحام شبكة المعلومات.[1]

3/- أنواع الجرائم الالكترونية:

أ/- الاحتيال الالكتروني:

هو استخدام غير مرخص لبيانات من قبيل أي شخص غي حامل للبطاقة الأصلية بهدف الحصول على بضائع أو خدمات وهذا الاستخدام قد يتطلب استخدام بطاقات حقيقة أو ما يتطلب ذلك منذ أن حققت شبكة الانترنت انتشارا عالميا دخلت عليها عمليات الاحتيال والنصب من أبواب مختلفة وكانت أشكال الاحتيال الأولى في مواقع الانترنت بعدها انتقلت إلى وسائل الدفع الالكتروني معتمدا على بساطة الناس وعقوبة تعاملهم مع سواهم والمبالغ التي يتم الاستيلاء عليها قد تصل إلى مئات ملايين الدولارات وخصوصا عندما يمنح احدهم رقم حسابه المصرفي لشخص عبر البريد الالكتروني وتنتشر مراكز عمل المحتالين في البلدان ، التي تنخفض فيها الرقابة على النشاط ألمعلوماتي وخصوصا في إفريقيا. [2]

ب/- التشهير:

لغة: شهره شهرا وشهرة أعلنه وأذاعه ،وشهر به أذاع عنه السوء وجعله معروفا به بين الناس.

اصطلاحا: الاعتداء على سمعة أحد بذكره سوء لدى عدة أشخاص أو عن طريق الصحف أو غيرها من طرق العلانية .[3]

والتشهير **Libel**من جرائم البث المباشر في القانون ، وهو في كل الأحوال نوع من القذف ، وإن كان يستلزم في القانون الأمريكي أن يكون كتابا ، في حين أن التشهير بالكلام يطلق عليه في المصطلح

---

[1]-شفيقة خنيفر،المؤتمر العلمي الافتراضي الأول: الجريمة الالكترونية (الواقع والتحديات) عنوان المداخلة الاجرام الالكتروني، كفاءات ضائعة في عالم التقنية ، جامعة محمد الشريف مساعديه ، سوق أهراس ،ص 2 ،3 .

[2]- سامر سلمان الجبوري ، جريمة الاحتيال الالكتروني ، منشورات زين، الحقوقية ، بيروت لبنان ، الطبعة الأولى 2018- ص18.

[3]- طارق عفيفي ،صادق أحمد ، الجرائم الالكترونية (جرائم الهاتف المحمول) ، الطبعة الأولى 2015 - ص ص167، 168.

الأنجلوفونيSlander . فالأساس الذي يعتمد عليه التشريع الأمريكي في إطار التشهير ، ينطلق من تهديد سمعة شخص ماMan's Réputations التي تمثل المصلحة التي يحميها القانون هنا.

وهو ذات الأمر في القانون الفرنسي فالمادة (R-624-3) من قانون العقوبات الفرنسي الجديد تنص على أنه القذف غير العلني يقع في مواجهة شخص أو مجموعة أشخاص بسبب أصلهم أو انتمائهم أو عدم انتمائهم ، الحقيقي أو المفترض إلى عرق أو أمة أو جذر أو دين. [1]

ج/- الاختراق:

هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف.وحينما نتكلم عن الاختراق عموما فنقصد بذلك قدرة المخترق على الدخول إلى جهاز آخر فهو مخترق أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب ويوجد ثلاثة أنواع من المخترقين.النوع الأول هم ما يسمى بأصحاب القبعات البيضاء وهذا النوع من المخترقين يقوم بمساعدة الناس ويعرف بالمخترقين الأخلاقيين .والنوع الثاني ما يسمى بأصحاب القبعات السوداء وهم مخترقين غير أخلاقيين يقومون بأعمال تخريب، والنوع الثالث هم أصحاب القبعات الرمادية، حيث يقومون بأعمال أخلاقية ، وفي نفس الوقت يقومون بأعمال تخريبية. [2]

د/ القذف:

لغة:هو الرمي من بعد – فمكان قذف وقذوف وقذيف بمعنى بعيد– والنفاذق : الترامي ، وقيل : الرمي بالعيب، والسب والشتم وورد في القرن قوله تعالى: "بل تقذف بالحق على الباطل فيدعمه فإذا هو زاهق"[3] وقوله تعالى : (لأرجمنك) [4]

---

[11]–عبد العال الديبري، الجرائم الالكترونية ، المركز القومي للأصادرات القانونية .الطبعة الأولى 2012 . ص 276.

[2]–http:/ : ar.Wikipedia .org

[3]–سورة الأنبياء ، الأية 18.

[4]– سورة مريم ، الأية 46.

شرعا: فعلى الرغم من اختلاف لفظ الفقهاء في تعريفهم لهذه الجريمة (القذف) وفي نطاق هذه الجريمة. كاختلافهم حول اعتبار الشهادة بالزنا قذفا من عدمه–إلا أنهم اتفقوا على أن القذف هو " الرمي بالزنا أو اللواط" .وبالتالي فإنه يخرج من مفهوم القذف– الموجب للحد– الرمي بكل معصية آخري غير الزنا كالسب والشتم ونحوهم.

تشريعا: نجد أن المشرع المصري قد عرف في المادة (302/1) من قانون العقوبات القاذف بأنه: يعد قاذفا كل من اسند لغيره بواسطة احدى الطرق المبينة بالمادة 171 من هذا القانون أمورا لو كانت صادقة لأوحيت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانونا او أوحيت احتقاره عند أهل وطنه".

أما المشرع السعودي فلم يورد صراحة في نظام مكافحة الجرائم المعلوماتية جريمة القذف، وإن كانت هذه الجريمة تخضع للمادة الثالثة من هذا النظام إذا تضمن البند (5) من هذه المادة "التشهير بالأخرين ، وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة [1].

هـ/ -<u>السب:</u>

لغة: السب هو الشتم بإطلاق اللفظ الصريح الدال عليه، بمشافهة الغير بما يكره، و(المسب) كثير السباب.

اصطلاحا: فقد عرف بعض الفقه السب بأنه " خدش شرف شخص أو اعتباره عمدا، بإلصاق صفة عيب أو لفظ جارح أم مشين إليه" وهوا ما يتفق مع تعريف جانب من الفقه الشرعي لذات الفعل ، إذ عرف ابن عابدين السب بأنه: نسبة المرء إلى فعل اختياري محرم شرعا ويعد عارا عرفا".

4/- أنماط الجريمة الالكترونية:

تتعدد أنماط الجريمة الالكترونية حسب نوع الفعل والوسيلة وكذا المحتوى والهدف ، يمكن إدراجها ضمن أربعة فئات رئيسية:

[1]– طارق عفيفي صادق أحمد ، الجرائم الالكترونية جرائم الهاتف المحمول ، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي ،محاضر منتدى بجامعة حلوان عضو الجمعية المصرية للاقتصاد السياسي والتشريع عضو الجمعية –المصرية للقانون الدولي–القاهرة– الطبعة الأولى 2015–ص ص 155– 156.

- جرائم مادية تدخل في إطار سرقة الرصيد ووسائل الاحتيال المتعلقة بتحديث البيانات.
- جرائم ثقافية تتعلق بسرقة المعلومات وحقوق الملكية الفردية.
- جرائم جنسية تقع تحت طائلة الاستدراج ونشر الصور الإباحية والتغرير وغيرها.
- جرائم سياسية واقتصادية تدخل في حيز نشر السلوك الخاطئ "نشر الإشاعات، الإرهاب الالكتروني".

خلص تقرير مكتب الأمم المتحدة المعني بالمحذرات والجريمة، في دراسته للجريمة السيبرانية إلى تحديد الأفعال التي تشكل الفعل الإجرامي المتعلق بالجريمة الالكترونية [1]،والذي ضمنه ثلاث فئات رئيسية يمكن توضيحها في الجدول الأتي:

الأفعال ضد السرية والنزاهة وتوافر بيانات الحاسب أو النظم

- الدخول غير المشرع لنظام الحاسوب.
- الدخول غير المشروع.
- الاعتراض غير المشروع للاتصالات.
- التدخل غير القانوني.
- التدخل غير القانوني.

أفعال ذات الصلة بالحاسوب لمصالح شخصية أو مادية أو أذى

- انتهاك الخصوصية.
- الاحتيال أو التزوير.
- جرائم الهوية "انتحال الهوية الالكترونية"
- الجرائم المتعلقة بحقوق النشر والعلامات التجارية.
- رسائل البريد الالكتروني الطفيلة.

[1]-- سواكري الطاهر وآخرون، نمطية الجريمة في المجتمع الجزائري ،مخبر الجريمة والانحراف بين الثقافة والتماثلات الاجتماعية، أ فريل 2022، ط1 ص234.

أعمال ذات الصلة بالحاسوب تسبب ضرر شخصي.

- استغلال الأطفال في المواد الإباحية.
- الأفعال ذات الصلة بمحتوى الحاسوب.
- أفعال ذات الصلة بالحاسوب تنطوي خطاب الكراهية والعنف والعنصرية.
- استدراج أو مراودة الأطفال " المواد الإباحية عن الأطفال المتعلقة بالحاسوب"
- أعمال ذات الصلة بالحاسوب في دعم جرائم الإرهاب."الإرهاب السيبراني".

ضف إلى ذلك خلصت اللجنة الاقتصادية والاجتماعية لغربي آسيا اسكو ESCWA إلى تفصيل كل فعل يعتبر جريمة الكترونية منها :جرائم الإساءة للأديان ، التشهير والابتزاز، المطاردة السيبرانية، العاب المقامرة على الحط التي تجرمها بعض الدول إذا ما ارتبطت بالمشاركة القسرية والاحتيال وسوء استخدام من قبل القصر ، التحرش الجنسي السيبراني...إلخ.[1]

5/- الأسباب الدافعة إلى ارتكاب الجريمة الالكترونية:

تتعدد أسباب الجرائم الالكترونية ، ويمكن أن تعزى إلى مجموعة واسعة ومتنوعة من العوامل النفسية والاجتماعية والتكنولوجية، وتعتبر هذه العوامل متداخلة ومعقدة ، حيث تؤثر كل منها على الأخر وتساهم في تفشي هذه الظاهرة بشكل متزايد في المجتمعات الحديثة ، وفيما يلي بعض من الأسباب الرئيسية التي يمكن من خلالها فهم أسباب الجريمة الالكترونية وتأثيرها على الأفراد والمجتمع ككل.[2]

لا تختلف الأسباب الدافعة إلى ارتكاب الجريمة الالكترونية عن باقي أنواع الجرائم الأخرى ومن أبرزها:

أ/-الدوافع الذاتية: والتي تجعل من الشخص يقوم بارتكاب عدد من المخالفات نابعة من حب الاستطلاع والتحدي والرغبة في قهر النظام المعوماتي واثبات الذات.

ب/-الدوافع النفسية: وتكون من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك.

ت/-الدوافع الاجتماعية:وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين.

---

[1]- سواكري الطاهر وآخرون، مرجع سابق ،ص ص235 ،236.

[2]- http://www.maktabtk.com

ث/-الدوافع المالية:(الربح وكسب المال): وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من أجل تحقيق المكاسب المالية.

ج/- الدافع السياسي والعسكري:التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الحاسوب،وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.

د/- الدافع القومي والوطني: وهو أن يقوم الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو تغيير أو تغيير هذه المواقع،مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع.[1]

[1]- محمد عبد السلام و، عادل محمد الشربجي: الجريمة الالكترونية في الفضاء الالكتروني المفهوم- الأسباب- سبل مكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات سداسية ، العدد 04، سنة 2019،ص 249.

المبحث الثاني:عمليات النصب والاحتيال عبر مواقع التواصل الاجتماعي.

1/- ماهية النصب والاحتيال في مواقع التواصل الاجتماعي.

أ/- مفهوم النصب والاحتيال عبر مواقع التواصل الاجتماعي:

يقع النصب والاحتيال بإرسال رسالة إلى شخص على الماسنجر أو البريد الالكتروني يدعم فيها مرسلها أن المرسل إليه كسب ثروة ، أو ميراث ، أو فاز في مسابقة ، وأن البنك يحتاج إلى رسوم مصرفية يتعين دفعها ، فهو الاحتيال الالكتروني عبر الانترنت لايمكن حصرها.[1]

ب/- تعريف النصب والاحتيال في الأنترنت:

تعتبر جريمة النصب والاحتيال في الانترنت internet raud أو ما يصطلح عليها جريمة الاحتيال المعلوماتي أشد أو أكثر الأموال المتداولة والمنتشرة عبر الشبكة إذا أنها تحتل المرتبة الأولى في العالم الافتراضي على عكس ما هو متعارف عليه في العالم المادي أين تتسيد جريمة السرقة وجرائم الأموال.[2]

أصبحت جرائم الاحتيال وطرق النصب عبر الانترنت متعددة أو مختلفة كانتحال اسم كاذب أو صفة غير حقيقية ، أو إيهام الناس بوجود مشاريع كاذبة ، أو إحداث الأمل بحصول ربح وهمي. [3].

---

[1]- دينا عبد العزيز فهمي – "المسؤولية الجنائية الناشئة عن استخدام مواقع التواصل الاجتماعي" : مجلة الحقوق للبحوث القانونية والاقتصادية ،م3، المجلد 2019 ،2،العدد2 يوليو 2019 ، ص 315.

[2]- مهدي ربوح ، زكرياء العيشي ، العوامل المؤدية لوقوع جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي الفايسبوك نموذجا،مذكرة مكملة لنيل ما ستر في تخصص علم الاجتماع الانحراف والجريمة ،كلية العلوم الاجتماعية والإنسانية ، جامعة الكلي محمد او لحاح بالبويرة ، سنة 2021-2022 ص 45.

[3]- عباس زكرياء ، ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي .
مذكرة مقدمة لنيل شهادة ما ستر في علم الاجتماع الانحراف والجريمة ، جامعة الجيلالي بونعامة خميس مليانة ، سنة 2022-2023 ص .

وصور النصب والاحتيال عبر الانترنت الأكثر انتشارا هي النصب ببطاقات الائتمان ويكون إما من حاملها الشرعي أو من الغير، أو عن طريق البريد الالكتروني ، ويعد هذا الأخير أشهر الخدمات التي تقدمها الانترنت إذ يجري بواسطتها إرسال واستقبال الرسائل الالكترونية، وقد شاع استخدام البريد الالكتروني بسبب سهولة إرسال الرسائل واستقبالها وقلة التكاليف وقصر الوقت كل هذا أدى إلى زيادة وتكاثر الرسائل الالكترونية المقلدة والمزورة.

لقد جرمت مختلف التشريعات العربية والأجنبية جريمة النصب ومن بينهم المشرع الجزائري الذي تناولها من خلال المواد 372-376 من قانون العقوبات أن يكون موضوع الاحتيال مالا وماديا ، سواء كان هذا المال منقول أو عقارا ، وأن يكون هذا المال مملوكا للغير إضافة إلى وجوب عناصر الركن المادي المتمثلة في السلوك الإجرامي بالطرق الاحتيالية وهي اتخاذ اسم كاذب أو صفة غير صحيحة أو الاحتيال بطرق التصرف في مال منقول أو عقار ليس مملوك للجاني ولكنه لم يغترف صراحة على وقوع جريمة النصب الواقع على الأموال عبر الانترنت من خلال المادة 394مكرر 1و2 .[1]

ت/-تعريف جريمة النصب والاحتيال في القانون الجزائري:

تعد جريمة النصب والاحتيال من الجرائم الخطيرة التي عايشها المجتمع حديثا كون هذه الجريمة حديثا كون هذه الجريمة لم يكن لها وجود قديما، وتبرز خطورة هذه الجريمة في إرباك الحياة الاجتماعية للأفراد خاصة وأن تأثيرها ينصب على مال يسلب من المجني عليه مما يؤدي إلى إخلال بالثقة بينهم،الأمر الذي ينعكس سلبا على المعاملات،وبالتالي تهتز القيم الأخلاقية وأيضا الاقتصادية ، ونظرا لهذه الخطورة تبنى المشرع الجزائري سياسية لمكافحتها من خلال تجريم السلوكيات التي تشكل جريمة نصب واحتيال ورصد مجموعة من العقوبات المناسبة لها وهو ما سنتطرق له تباعا من خلال الأتي:

نصت المادة "372"من قانون العقوبات على مايلي:

" كل من توصل إلى استلام أو تلقي أموال و منقولات أو سندات أو تصرفات أو أوراق مالية أو ووعود ومخالصات أو إبراد من الالتزامات أو الحصول على أي منهما وكان كذلك بالاحتيال لسلب كل ثروة

[1]-بوكساني شيراز وسرحان شيماء : جريمة النصب والاحتيال عبر مواقع التوصل الاجتماعي ، مذكرة لنيل شهادة ما ستر في القانون ، كلية الحقوق بودواو ، جامعة احمد بوقرة – بومرداس ، 2023/2022 م ص 12.

الغير أو بعضها أو الشروع فيه باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي بإحداث الأمل في الفوز بأي شيء أو وقوع حادث أو أية واقعة أخرى وهمية يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة مالية من 5000 دج إلى 20000دج.[1]

[1]– لموشي جهيدة ، طالبة دكتوراه، دور الضحية في حدوث الجريمة النصب والاحتيال –مقاربة سوسيولوجية ، كلية الآداب والعلوم الإنسانية والاجتماعية ، جامعة باجي مختار عنابة .ص ص252–253

2/-أركان جريمة النصب والاحتيال:

- **الركن الشرعي:** يتمثل الركن الشرعي في هذه الجريمة في نص المادة 372 من قانون العقوبات

والتي سبق التطرق لها أعلاه ومن خلال هذه المادة نجد أن المشرع الجزائري نص على تجريم السلوكات التي تدخل ضمن نطاق عمليات النصب والاحتيال، كما نص على العقوبات المقررة لها في حال وقعت الجريمة وهذا تطبيقا لنص المادة الأولى من قانون العقوبات التي تنص على انه لا جريمة ولا عقوبة ولا تدبير آمن بغير نص .

- **الركن المادي:** يتمثل الركن المادي في هذه الجريمة من:

أ/- استعمال أحدى وسائل التدليس: والهدف من ذلك أخذ مال الغير طواعية وبكل رضا باستعمال إحدى وسائل التدليس التي تتمثل في استعمال أسماء أو صفات كاذبة أو الادعاء بعمل في وظيفة معينة أو غداء بوجود قرابة عائلية مع شخص ما أو الادعاء بالحصول على شهادة علمية أو شرفية أو بوجود علاقة قانونية أو باستغلال صفة حقيقة و غيرها من الوسائل الاحتيالية .

ب/- الاستيلاء على مال الغير:أي تحقق النتيجة الإجرامية وهو ثاني عنصر من عناصر الركن المادي في هذه الجريمة وحسب ما ورد في نص المادة 372 من قانون العقوبات سالفة الذكر فإن المال محل الجريمة يتمثل في الأموال مهما كانت طبيعتها سواء سائلة أو منقولة أو السندات أو التصرفات أو الأوراق المالية أو الوعود والمخالصات والإيرادات من الالتزامات.

ج/ العلاقة السببية: لاكتمال الركن المادي للجريمة يشترط توفر العلاقة السببية بين سلب مال الغير وبين الطرق الاحتيالية التي لجأ لها الجاني فإذا انقطعت هذه الرابطة لا يقوم الركن المادي وبالتالي تنتفي الجريمة ، ويتحقق ذلك لو أن المجني عليه توهم أن الشخص يعده فيقدم له أموالا مقابل القيام بأمر ما فهنا لا تقوم الجريمة لانعدام الرابطة بين كلام المتهم وبين ما توهمه الضحية والتي على أساسها سلم أمواله له.[1]

- **الركن المعنوي:**تتطلب هذه الجريمة توفر القصدين العام والخاص، ويقصد **بالقصد الجنائي العام:**

[1]جريمة النصب والاحتيال في القانون الجزائري ،محاضرة ، شوهد يوم 2025/05/20، على الساعة 10.00،ص03 moodle.université-eltarf.dz

علم الجاني بالعناصر المتمثلة في ماديات الجريمة وانصراف إرادته إلى تحقيق هذه العناصر ،وذلك بأن ينصرف الجاني للقيام بالتدليس لحمل المجني عليه على تسليم ماله ما يشترط أن يكون الجاني على علم ومدرك أن المعلومات التي يقدمها للضحية معلومات كاذبة مع اتجاه إرادته لسلب مال الغير وتملكه .

أما القصد الجنائي الخاص فيتمثل في نية الجاني في الاستيلاء على مال المجني عليه كله او بعضه ، فان لم تتوفر له نية التملك فلا يسال جزائيا لانتفاء عنصر القصد الخاص كمن يحتال ويتسلم شيئا لينتفع به مدة معينة من الزمن ثم يرده ففي هذه الحالة انتفى القصد الخاص فلا تقوم جريمة النصب وإنما تقوم جريمة أخرى مثل استعمال مال الغير على نحو غير شرعي أو بدون وجه حق .[1]

3/- العوامل المؤدية لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي:

إن من أهم أسباب انتشار جرائم الحاسب الآلي صعوبة اكتشاف هذه الجرائم مقاضاة المتهم لأنه لا يوجد في أغلب الأحوال شاهد للقضية ولا دلائل يمكن استخدامها للتواصل إلى المجرم وقد سهل انتشار شبكة الانترنت في الآونة الأخيرة على مستوى عالمي اختراق نظم المعلومات المرتبطة بالشبكة من قبل قراصنة المعلومات الذين يقبعون في أماكن بعيدة لم تكن تشكل خطرا في السابق لانعدام الوسيلة ولاحظ"سكوت سارني" المسؤول عن مكافحة الجريمة على الإنترنت في وزارة العدل الأمريكية أن الكمبيوتر الموصول بشبكة الإنترنت يسهل الجريمة أيضا على غرار دعارة الأطفال .واعترف "دوغلاس بيرت"،أحد المسؤولين في مركز الحماية من جرائم الحاسب الألي التابع للشرطة الفيدرالية الأمريكية بأنه: لا يمكننا أن نتوقع كل شيء لأن تحديد الخطر أمر بالغ الصعوبة علاوة على ذلك، يمكن أن نضيف عددا أخر من الدوافع وراء انتشار جرائم تكنولوجيا المعلومات منها:

- الفرص المتزايدة: إن ازدياد عدد مستخدمي الحاسوب من ذوي المعرفة والمقدرة في اختراق البيانات

نتيجة " لامركزية والمتلاعبين لتنفيذ أغراضهم لاسيما في ظل سيطرة ورقابة غير كفنة في هذا المحيط الإلكتروني لمعالجة البيانات.

[1] جريمة النصب والاحتيال في القانون الجزائري ، نفس المرجع ص03

- صعوبة الاكتشاف: إن وجود كم كبير من البيانات المخزنة ف الحاسوب يجعل إخفاء أي تزوير أو تلاعب عملية سهلة خاصة إذا تمكن مرتكب الجريمة من عدم ترك أي دليل خلفه الأمر الذي يترتب صعوبة اكتشاف الجريمة.
- تحقيق أرباح كبيرة: نتيجة للأرباح الطائلة التي يمكن أن يجنبها مرتكب التزوير والتلاعب فإنها

تشكل دفاعا قويا لأصحاب النوايا السيئة في ارتكاب جريمتهم في استبيان إجراء أحد الباحثين في أمريكا عام 1995 بين أن معدل أرباح مرتكب جريمة الحاسوب وصلت إلى 600.000 دولار مقابل 300.000 دولار لمرتكب الجريمة في النظام التربوي.

- الدوافع الشخصية :غالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالقوة والذات وبقدرته

على اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات ومن أجل تأكيد قدرته الفنية على ارتكاب أحد جرائم الكمبيوتر وقد يكون الهدف من ارتكاب الجريمة الحقد والكراهية.

- الدوافع الذهنية أو النمطية: الصورة الذهنية لمرتكبي جرائم الحاسب الآلي والانترنت غالبا هي

صورة البطل والذكي الذي يستحق الإعجاب، لا صورة المجرم الذي يستوجب محاكمته فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقائهم ببراعتهم.

- حب المغامرة و الإثارة:جاء على لسان أحد القراصنة في كتاب أنظمة الكمبيوتر كانت القرصنة هيالنداء الأخير الذي يبعثه دماغي .
- صعوبة الاحتفاظ بأثرها إن وجدت.
- تحتاج إلى خبرة فنية وتقنية ويصعب على المحقق التقليدي التعامل معها.
- تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- تعتمد على قمة الذكاء والمهارة في ارتكابها.[1]

4/- دور الضحية في حدوث جريمة النصب والاحتيال:

باعتبار أن الضحية هي أحد الأركان الفعل الإجرامي فإن الضحية في كثير من الحيان لا تخلو من دور الذي تلعبه في حدوث الجريمة ،وتوضح دور الضحية في وقوع الجريمة له أهمية بالغو على صعيد

[1]- جريمة النصب والاحتيال في القانون الجزائري ،نفس المرجع ص 50.

وقاية الضحية المحتملة من الانزلاق في الجريمة ، لأن فهم سلوك الضحية والدور الذي يلعبه في تهيئة الفرصة الإجرامية سوف يساعد أجهزة مكافحة الجريمة على اتخاذ التدابير الوقائية المناسبة لمواجهة الجريمة والحيلولة دون وقوعها.

أ/- دور الضحية في بث فكرة الجريمة لدى المجرم :

يقرر علماء الإجرام أن هناك قوتان تتصارع في نفس المجرم ، القوة الأولى هي قوة الدافع إلى ارتكاب الجريمة والثانية هي قوة المانع من الجريمة ويقرر علماء إن الضحية يأتي بتصرفات ما يجعل الجريمة في نظر مرتكبها غير مستنكرة ، فيقل المانع من الجريمة في نفس المجرم وهي فكرة لا تنشأ من فراغ بل هي نتيجة إيحاءات ومؤثرات خارجية تتكاثف ولعل أهم هذه المؤثرات ما يتعلق بشخصية الضحية وما تنطوي عليه سمات تجعلها قابلة للوقوع ضحية للجريمة، كالضحية التي تتباهى بممتلكاتها أمام الآخرين فهي بطريقة غير مباشرة تخلق فكرة الجريمة لدى النصاب حتى يحتال عليها.

ب/- دور الضحية في توفير الفرصة المناسبة:

تساعد الضحية في كثير من الأحيان في توفير الفرصة الملائمة للمجرم حتى يقوم بنصب والاحتيال عليها،وذلك من خلال التقصير أو الإهمال واللامبالاة وعدم الحفاظ على ممتلكاته أو التسرع في أخذ القرارات مما يتيح الفرصة أمام كل من لديه استعداد إجرامي، والنصاب يختار ضحيته من خلال ضعفها واحتياجها في شيء ما.نأخذ على سبيل المثال حاجة الضحية للسكن تمثل فرصة مناسبة للمجرم حتى يحتال عليه ويسلبه ماله ،كما إن غياب مصدر الحماية يلعب دورا هاما في وقوع الجريمة على بعض الأفراد الأمر الذي يسهل عمل المجرم ويتيح أمامه الفرصة المناسبة لعمله الإجرامي ، فد برهنت العديد من الدراسات والأبحاث إن معظم مرتكبي الجرائم يفضلون ارتكاب جرائمهم في المكان الذي يفتقر إلى الحماية .فالمرأة الغنية التي تعيش لوحدها من دون حماية يمكن لها أن تتعرض لمجرم نصاب يحتال عليها كونها هدف سهل من دون حماية يغري كل من لديه استعداد إجرامي.

ج/- دور الضحية في حدوث الجرائم المستحدثة:

وهي الجرائم الخفية التي لا يتم الإبلاغ عنها ولاتصل إلى الشرطة ، نظرا لأسباب عديدة منها عدم رغبة الضحية في المثول أمام الشرطة والمحاكم، أو لحساسية الجريمة وتعلقها بشرف العائلة ،أو لعدم وجود

وقت كاف لدى الضحية لمتابعة القضية ،أو قناعة الضحية بأنه حتى ولو تمكن إبلاغ الشرطة عن الجريمة التي حددت له فإنها لا تتخذ الإجراءات اللازمة والكفيلة لاسترجاع حقوقها والقبض على المجرم.

د/- ضحية ليس لها دور في الجريمة:

في بعض جرائم النصب والاحتيال لا يمكن لضحية أي دور فيما وقع عليه من اعتداء، كأفراد الذين يحذرون من ارتكاب الممارسات السلوكية الخاطئة، ويحرصون على ممارسة السلوك السوي،كما يتخذوا كافة التدابير لحماية أموالهم وممتلكاتهم ويتعدون عن المواقع المحتملة لحدوث الجريمة، مثال على ذلك حيث لا يكون دور فيما وقع عليه من اعتداء.[1]

5/العقوبات المقررة في جريمة النصب والاحتيال في القانون الجزائري:اعتبر المشرع الجزائري أن توجيه الطرق الاحتيالية لخداع الجمهور ظرفا لما قد ينجم عنه من نتائج خطيرة وضارة تهدد المجتمع وتصيب الاقتصاد الوطني وعلى ذلك نصت المادة 372فقرة 2 من قانون العقوبات الجزائري "وإذا وقعت الجنحة من شخص لجا إلى الجمهور بقصد إصدار أسهم أو سندات أو أذنات أو حصص أو أية سندات مالية سواء للشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى 10 سنوات والغرامة إلى 4000.00 د ج ".

يظهر لنا من خلال هذه الفقرة أن المشرع نص على ظرف واحد مشدد للعقوبة في جريمة النصب ،ويتمثل هذا الظرف المشدد في لجوء الجاني إلى الجمهور بهدف الاستيلاء على أمواله .وهذا ما سيتبين في المطلب الأول

المطلب الأول: عقوبات في حالات الجنحة

تقضي القواعد العامة وجوب القول بأن تمام يكون بتسليم مال الذي سعى الجاني باحتياله إلى الاستيلاء عليه إذ إن التسليم يمثل الهدف الذي يستهدفه الجاني لتمام الجريمة ،فهي تبدأ باستعمال الطرق الاحتيالية وتنتهي بالتسليم.

[1]جريمة النصب والاحتيال في القانون الجزائري،نفس المرجع ص ص 50 /51.

لقد كان القانون الفرنسي في ظل المادة 405 من قانون العقوبات فرنسي يعاقب على جريمة النصب بتحقق الضرر للمجني عليها أي بسلب كل أو بعض ثروته، وليس بتحقق فعل التسليم ،وبتعديل 1863 عدل المشرع الفرنسي صياغته المادة 405، ربط بين فعل التسليم وتمام جريمة النصب.[1]

حدد المشرع الجزائري العناصر المكونة لجنحة النصب في الفقرة الأولى من نص المادة إلى لعقوبة المقررة لها وحدد العقوبة المقررة لها وحدد العقوبة الأصلية والتكميلية التي سنتطرق لها في الفروع الآتية:

الفرع **الأول: العقوبات الأصلية**

التي نصت عليها في المادة 372 من قانون العقوبات على العقوبة الأصلية لجريمة النصب كالتالي "يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة مالية من 20000 إلى 10000د ج ،يعاقب الجاني الذي ارتكب جريمة النصب ضمن العناصر للأركان التي ذكرناها سابقا من ركن مادي وركن معنوي بالعقوبات التالية :

1-الحبس من سنة على الأقل إلى خمس سنوات

2-والغرامة المالية المقدرة ب20000 إلى 100000د ج.[2]

تجدر الإشارة إلى أن المشرع أشار إلى أنه يجب الحكم على المتهم بعقوبة الحبس والغرامة معا ، أي أنه يجب على القاضي الجمع بين العقوبتين في حكم واحد.

كما يمكن للمحكوم عليه أن يستفيد من نص المادة 53 مكرر 4 من ق.ع.ج " إذا كانت العقوبة مقررة قانونا في مادة الجنح هي الحبس / أو الغرامة ،وتقرر إفادة الشخص الطبيعي غير المسبوق قضائيا بالظروف المخففة ،يجوز تخفيض عقوبة الحبس إلى شهرين والغرامة إلى 20000دج....."

لقد أورد المشرع الجزائري في جريمة النصب غرامة مالية محددة بين الحد الأدنى والحد الأقصى فلا يمكن تجاوزها،وتتمثل في إلزام المحكوم عليه بدفع مالي لا يقل عن حد معين ولا يزيد.

---

[1]- باعلي حفيظة :جريمة النصب في ظل قانون العقوبات الجزائرية ،مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق ، تخصص قانون الجنائي ،كلية الحقوق والعلوم السياسية جامعة غرداية ،سنة 2018/2017 م ص ص 82-83 .

[2]-قرار صادر، يوم 17 ديسمبر 1966 من الغرفة الجنائية نشرة وزارة العدالة لسنة 1968 ،ص 65.

كما أن هذه العقوبة لا يقتصر تطبيقها على جريمة النصب التامة فقط بل تطبق أيضا على الشروع فيها أي محاولة نصب ثروة الغير، ولقد عبر عنها المشرع في نص المادة 372. "كل من توصل إلى استلام أموال .....أو شرع في ذلك....."[1].

يظهر أيضا هذا النص أن المشرع الجزائري جعل عقوبة الشروع في جريمة النصب نفسها عقوبة جريمة النصب تام .

بينما نجد المشرع الفرنسي في نص المادة 313 -1 حدد عقوبة جريمة النصب بالحبس لمدة خمس سنوات ، وبغرامة مالية تقدر ب 375000 أورو ، تجدر الملاحظة إلى أن المشرع الفرنسي شدد عقوبة الغرامة المالية بنسبة لجريمة النصب بالمقارنة مع المشرع الجزائري وهذا ما يجعل العقوبة أكثر ردعا .

الفرع الثاني: العقوبة التكميلية.

إضافة إلى العقوبة الأصلية المنصوص عليها في مادة 372 من ق.ع.ج ، نص المشرع الجزائري في الفقرة الثالثة من نفس المادة على عقوبة أخرى وهي العقوبة التكميلية كما جاء فيه "وفي جميعا الحالات يجوز أن يحكم علاوة على ذلك على جانب الحرمان من الحقوق الواردة في المادة 14 ق.ع.ج أو بعضها وبالمنع من الإقامة وذلك لمدة سنة على الأقل إلى خمس سنوات على الأكثر"يستفاد من هذه الفقرة أن العقوبة هيا عقوبة ذات طابع جوازي ، أي يجوز للقاضي الحكم بها أو الاستغناء عنها تماما وتتمثل هذه العقوبة في الحكم بالحرمان من جميع أو بعض الحقوق الوطنية .

ولمعرفة هذه الحقوق ،فقد أحالتنا المادة 372من قانون العقوبات الجزائري في فقرتها الثالثة إلى المادة 14 من قانون العقوبات الجزائري التي نصت على "يجوز للمحكمة عند قضائها واردة في المادة 14 ق.ع.ج

أو بعضها وبالمنع من الإقامة وذلك لمدة سنة على الأقل إلى خمس سنوات على الأكثر يستفاد من هذه الفقرة أن العقوبة هي عقوبة ذات طابع جوازي،أي يجوز للقاضي الحكم بها أو الاستغناء عنها تماما وتتمثل هذه العقوبة في الحكم بالحرمان من جميع أو بعض الحقوق الوطنية.

1- الحرمان من حق الانتخاب والترشح ومن حمل أي وسام .

[1]- لحسن بن شيخ :مذكرة القانون الجزائي الخاص ،الجرائم ضد الأشخاص والجرائم ضد الأموال ،دار هومة للطبعة والنشر والتوزيع، الجزائر، سنة 2012 ص 202.

2- عدم الأهلية لأن يكون مساعدا محلفا ،أو خبيرا ، أو شاهدا على أي عقد ، أشاهدا أمام القضاء إلا سبيل الاستدلال .

3- الحرمان من الحق في حمل الأسلحة، وفي التدريس،وفي إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا ، أو مدرسا أو مراقبا .

4- عدم الأهلية لأن يكون وصيا أو قيما .

5- سقوط حقوق الولاية كلها أو بعضها .[1]

بالإضافة إلى الحكم على الجاني بالحرمان من هذه الحقوق الوطنية ، يجوز للقاضي لنص المادة 372 من قانون العقوبات الجزائري في الفقرة الثالثة الحكم بذلك بالمنع من الإقامة سنة إلى خمس سنوات على الأكثر .[2]

وتجدر الإشارة إلى تطبيق هاتين العقوبتين هو أمر جوازي، و تطبيقهما يكون بصدد تطبيق العقوبة الأصلية أو في حالة الظروف المشددة.

المطلب الثاني: عقوبات في حالات الجنحة المشددة

اعتبر المشرع الجزائري أن توجيه الطرق الاحتيالية لخداع الجمهور ظرفا مشددا لما قد ينجم عنه من نتائج خطيرة وضارة تهدد المجتمع وتصيب الاقتصاد الوطني ، وعلى ذلك نصت المادة 372 فقرة 2 من قانون العقوبات الجزائري وإذا وقعت الجنحة من شخص لجاه إلى الجمهور يقصد إصدار أسهم أو سندات أو أذنات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 400000دج.

يظهر لنا من خلال هذه الفقرة أن المشرع الجزائري نص على ظرف واحد مشدد للعقوبة في جريمة النصب، ويتمثل هذا الظرف المشدد في لجوء الجاني إلى الجمهور بهدف الاستيلاء على أمواله .

1- العقوبة في حالة الظروف المشددة:

لقد نص القانون للعقوبات الجزائري على ظرفين مشددين فيما يحص جنحة النصب:

---

[1]قرار صادر، يوم 17 ديسمبر 1966 من الغرفة الجنائية نشرة وزارة العدالة لسنة 1968نفس المرجع

[2]- باعلي حفيظة ، نفس المرجع ص86.

أولا: ظرف يتعلق بالجاني وهو الظرف المنصوص عليه في فقرة الثانية من المادة 382 مكرر من قانون العقوبات الجزائري .[1]

فيما يتعلق الظرف المتعلق بالجاني نص المشرع الجزائري في الفقرة الثانية من المادة 372 من قانون العقوبات الجزائري بجنحة النصب على النحو التالي "وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة 400000 دج."

لقد اعتبر المشرع أن توجيه 4الطرق الاحتيالية لخداع الجمهور ظرفا مشددا ، والعلة من وراء التشديد تكمن في الخطورة الإجرامية لشخصية الجاني وزعزعة ثقة الجمهور من خلال إصدار أسهم وسندات وما شابه ذلك مما يضر الاقتصاد الوطني.

إن توجيه أساليب الخداع إلى جمهور الناس يفترض أن يكون المحتال قد استعمل وسيلة العلانية أي بخطاب جمهور الناس ، داعيا إياهم إلى الاكتتاب في الأسهم أو السندات التي أصدرها ويراد بوسيلة العلانية كل أسلوب يتجه الخطاب فيه إلى عدد غير محدود من الناس فقد يكون النشر في صحيفة دورية أو توزيع منشورات في الطرق العامة أو لصق إعلانات على الجدران ، أو الجهر بالدعوة في مكان عام عن طريق الإذاعة أو التلفزيون.

ويقصد بإصدار أسهم أو سندات التي تصدرها شركة المساهمة والتي تستهدف بها جلب رأس مال جديد إلى الشركة سواء كانت في طور تأسيسها أو كانت موجودة بالفعل وتسعى إلى زيادة رأس مالها ،فقط تتضمن تأسيسي شركة وهمية أو تضمن مبالغة في تقدير أرباح شركة قائمة أو نشرت بهذه الطريق موازنة مزورة .[2]

أما بالنسبة للمشرع الفرنسي فقد رفع عقوبة جريمة النصب في حالة الظروف المشددة بموجب نص المادة 313 –02 من قانون العقوبات الفرنسي سبع سنوات حبس وغرامة مالية تقدر 750000 أورو وهذا في حالات محددة على سبيل الحصر بموجب نفس المادة سالفة الذكر ، والملاحظة الجديرة بالذكر

[1]– عبد الله سليمان :دروس في شرح قانون العقوبات الجزائري ، القسم الخاص ، دار هومة للطباعة والنشر والتوزيع ، الجزائر ، الطبعة الثانية ، سنة 1989، ص243.

[2]– باعلي حفيظة: مرجع سبق ذكره ،ص ص87–88.

هي أن حالات الظروف المشددة في نص المادة المتعلقة بجريمة النصب في قانون العقوبات الفرنسي هي متعددة بالمقارنة مع حالات الظروف المشددة في نص المادة 372 من قانون العقوبات الجزائري .[1]

ثانيا: أما فيما يخص الظرف المتعلق بالمجني عليه فقط نصت المادة 382 مكرر من قانون العقوبات الجزائرية أنه عندما ترتكب الجرائم المنصوص عليها في الأقسام الأولى والثانية والثالثة من الفصل الثالث من هذا الباب ضد الدولة أو الأشخاص الاعتبارية المشار إليه في المادة 119 فإن الجاني يعاقب :

1- بالسجن المؤبد في الحالات الواردة في المواد 352 و 353 و 354 .

2- بالحبس من سنتين إلى عشر سنوات إذا كان الأمر يتعلق بجنحة باستثناء الحالة التي تنص عليها المادة 372 من قانون العقوبات.

وتجدر الإشارة إلى أن المادة 119 من قانون العقوبات الجزائري تم إلغاؤها بموجب القانون رقم 06 -01 المؤرخ في 02/20 /2006 المتعلق بالوقاية من الفساد ومكافحته ، والتي تم تعويضها بالمادة 29 من نفس القانون . [2]

6/نصائح مهمة لتجنب الوقوع في النصب والاحتيال الالكتروني:

- **تحديث الأجهزة الرقمية باستمرار:**

ينبغي على المستخدمين تحديث أجهزتهم الرقمية بشكل مستمر، سواء كانت أجهزة حاسوبية أو خلوية، وذلك لإصلاح الثمرات والعيوب الأمنية التي يستغلها المجرم الالكتروني للوصول إلى المعلومات الشخصية والمالية. بما في ذلك تحديث أنظمة التشغيل ، والبرامج والتطبيقات، ومتصفحات الويب الموجودة على الجهاز.وفي حال استخدام البرامج الوقائية كالبرامج المضادة للفيروسات والحماية ، فمن الضروري تفعيل خيار التحديث التلقائي ، للوصول إلى أحدث الإصلاحات التي توفرها باستمرار.

- **الحذر من التصيد الاحتيالي:**

[1]-محمود نجيب حسني : شرح قانون العقوبات ،(القسم الخاص)، دار النهضة العربية ، القاهرة سنة 1988 ص399.

على الرغم من تعدد طرق الاحتيال الالكتروني وتزايدا باستمرار ، إلا أن التصيد الاحتيالي Phishing"عبر البريد الالكتروني هو أحد الطرق الأكثر شيوعا لوصول المجرم الالكتروني إلى هدفه ، وذلك من خلال إرسال رسائل بريد إلكتروني ضارة ، تبدو وكأنها من مصادر موثوقة ويتضمن محتواها طلب إرسال بعض المعلومات الشخصية من المستخدم ، أو النقر فوق رابط ما ليجرى الحصول على تلك المعلومات بشكل غير قانوني ثم استغلال الضحية واستخدامها ضدها في ما بعد .

- **استخدام كلمات مرور قوية:**

يمتلك المستخدمون حسابات عدة على مواقع مختلفة على شبكة الانترنت ، ويجب إنشاء كلمات مرور طويلة ومعقدة لكل حساب على حدة ، دون تكراره في أكثر من موقع ، حيث يجب أن تحتوي كلمة المرور على مجموعة من الأحرف والأرقام والرموز بحيث يصعب تخمينها والوصول إليها.

مع مراعاة عدم تضمين المعلومات الشخصية في كلمات المرور ، كما يجب المداومة على تغييرها بين فترة وأخرى والحرص على عدم مشاركتها مع أشخاص آخرين، أو حتى الاحتفاظ بها مكتوبة في أي مكان، كالاحتفاظ بها على ورقة مثلا .

- **الحفاظ على سرية المعلومات الشخصية :**

ينصح بإبقاء المعلومات الشخصية مخفية دائما ، وتجنب مشاركتها عبر مواقع التواصل الاجتماعي، لأن ذلك قد يوفر فرصة للمجرمين الالكترونيين للحصول عليها واستغلالها للوصول إلى نواياهم الخبيثة ، حيث يمكنهم استخدام معلومات تاريخ ميلاد وبعض المعلومات الشخصية الأخرى لاختراق كلمات المرور الخاصة بالحساب ، بالإضافة إلى ذلك يجب الحرص على عدم إضافة أي معلومة شخصية على المواقع الالكترونية قبل التأكد من صحتها وأمانها، مثل تقديم أرقام الحسابات وكلمات المرور وما إلى ذلك.

- **تفعيل ميزة** المصادقة **الثنائية:**

تعد المصادقة الثنائية "2Fa" خطوة مهمة لزيادة حماية بيانات المستخدمين، ومنع وصولالمتسللين والمجرمين الالكترونيين إلى حساباتهم أو أجهزتهم الخاصة، إلا تعمل كطبقة حماية إضافية في حال معرفة المحتالين بطريقة ما لكلمات المرور الخاصة بحسابات الضحايا.

إذ تتطلب المصادقة الثنائية تأكيد الهوية بطريقة أخرى لدخول الحساب الشخصي ، وليس فقط كلمة المرور، وذلك عن طريق بصمة الإصبع أو الوجه، أو إرسال رمز مؤقت "OTP" على الهاتف المحمول يجب إدخاله مع كلمة المرور ، وغير ذلك.[1]

7/ -إحصائيات:

الجدول 1: يبين نوع الجرائم المرتكبة خلال سنة 2022.

نوع الجرائم المرتكبة	المجموع	النسبة المئوية%
القذف	46	27.54
السب	16	9.58
التهديد	6	3.59
الابتزاز	5	2.99
انتحال الصفة	13	7.78
المساس بالحياة الخاصة	10	6
النصب	30	17.96
نشر محتوى مخالف للنظام العام	7	4.19
أخرى	34	20.36
المجموع	**167**	100

المصدر : أمن ولاية المدية

قراءة إحصائية تحليلية للجرائم المرتكبة سنة 2022:

[1] https://www.facebook.com/100066615885851/posts/1047149927515527/?mibExtiD=RS40AB7S9UCBXW6.

نلاحظ من خلال الجدول أن جريمة القذف تحتل المرتبة الأولى بنسبة 27.54 % ، وهو ما يعكس ارتفاع حالات التشهير في السمعة ، عبر وسائل التواصل الاجتماعي.

أما الجرائم المصنفة تحت " أخرى" تمثل نسبة كبيرة 20.36 % مما يشير إلى وجود أنواع مختلفة من الجرائم المتفرقة التي لم تصنف بشكل دقيق.

أما النصب جاء في المرتبة الثالثة بنسبة 17.96 % ، مما يدل على وجود مشاكل في الوعي المالي واستغلال الثقة .

بالنسبة لجرائم الابتزاز والتهديد رغم نسبتهما المنخفضة إلا أنهما يعكسان مظاهر من العنف النفسي أو المادي .

أما السب 9.58 % والمساس بالحياة الخاصة 6 % ونشر محتوى مخالف 4.19% كلها تشير إلى اختراقات لحرمة الأفراد ، وربما تأثرت بزيادة استخدام التكنولوجيا والفضاء الرقمي .

انتحال الصفة 7.78 % قد تكون مرتبطة بمحاولات خداع إلكترونية أو استغلال لسلطة مزيفة .

الجدول 2: يوضح نسبة الجرائم الالكترونية لسنة 2023:

نوع الجرائم الالكترونية	المجموع	النسبة المئوية%
القذف	55	22.92
التهديد	16	6.7
الابتزاز	17	7.08
انتحال صفة	7	2.92
المساس بالحياة الخاصة	7	2.92
نشر صور	17	7.08
تحريض على الفسق	1	0.42
نشر محتوى تحريضي	1	0.42
النصب	43	17.92
التحريض على الكراهية بين الناس	1	0.42
نشر محتوى مخالف لنظام العام	12	5
بيع منتجات محظورة	31	12.92
حالات اخرى	32	13.33
المجموع	240	100

المصدر: أمن ولاية المدية

قراءة إحصائية تحليلية للجرائم الالكترونية المرتكبة سنة 2023 :

نلاحظ من خلال الجدول أن جريمة القذف هي الأكثر انتشارا بنسبة 22.92 % ما يشر إلى ضعف الوعي القانوني والأخلاقي لدى بعض المستخدمين.

أما النصب بنسبة 17.92% حيث يشكل تهديدا واضحا ، مما يدل على وجود شبكات أو أفراد يستغلون الفضاء الرقمي في النصب المالي .

بيع منتوجات محظورة بنسبة 12.92% ، وأما الحالات الأخرى بنسبة 13.33 % .

والابتزاز والتهديد وانتحال الصفة والمساس بالحياة ونشر محتوى مخالف للنظام العام كلها تمثل من 2.92% إلى 7.08% رغما قلتها إلا أن خطورتها كبيرة لأنها تمس القيم الدينية والمجتمعية ومرتبطة بالمساس بالحياة الخاصة والخصوصية الرقمية.

أقل الجرائم انتشارا تحريض على الكراهية، نشر محتوى تحريضي ، تحريض على الفسق ، نشر صور فاضحة : فكل منها سجل حالة واحدة فقط بنسبة 0.42 % .

الجدول 3: يوضح نسبة الجرائم الالكترونية المرتكبة سنة 2024.

نوع الجرائم الالكترونية	التكرار	النسبة المئوية %
الدخول والبقاء عن طريق الغش	22	9.20
القذف	46	19.25
السب	11	4.60
التهديد	04	1.67
الابتزاز	07	2.93
انتحال الصفة	02	0.84
المساس بالحياة	15	6.27
نشر صور مخالفة للحياء	01	0.42
تحريض على الفسق	01	0.42
النصب	87	36.40
التحريض على الكراهية	05	2.09
نشر محتوى مخالف لنظام العام	08	3.35
حالات أخرى	30	12.55
المجموع	239	100

المصدر: أمن ولاية المدية

قراءة إحصائية تحليلية للجرائم الالكترونية المرتكبة سنة 2024 :

نلاحظ أن أكثر أنواع الجرائم شيوعا النصب بنسبة 36.40% يدل على أن الكثير من المستخدمين لا يزالون عرضة لأساليب خداع عبر الانترنت مثل الرسائل المزيفة والاحتيال المالي .

القذف تتمثل نسبته 19.25% مما يشير إلى سوء استخدام مواقع التواصل الاجتماعي وانخفاض الوعي القانوني والسلوكي في التفاعل الرقمي .

أما الحالات الأخرى تمثل 12.55%، توحي بوجود جرائم متنوعة غير مصنفة ما يستدعي تطوير تصنيف أكثر تفصيلا للجرائم الالكترونية، والدخول والبقاء عن طريق الغش 9.20 % ، المساس بالحياة الخاصة 6.27% . رغم نسبها أقل فهي تثير القلق كونها تؤثربعمق على الضحايا نفسيا واجتماعيا.

نشر محتوى مخالف للنظام العام وتحريض على الكراهية والابتزاز والتهديد والسب تتمثل نسبتهم : من 1.67 % إلى 3.35% .

أقل أنواع الجرائم حدوثا نشر صور مخالفة للحياء و التحريض على الفسق حالة واحدة لكل منهما 0.42%

خلاصة

تناولنا في هذا الفصل مبحثين المبحث الأول تطرقنا إلى مفهوم الجريمة الالكترونية باعتبارها أحد أخطر التحديات التي تواجه المجتمعات في العصر الرقمي،حيث ترتكب باستخدام التكنولوجيا الحديثة وخاصة الانترنت ،ونشأة الجريمة الالكترونية وتطورها مع التركيز على جرائم النصب والاحتيال الالكتروني التي تستهدف الإفراد ،و الأدوات والوسائل المستخدمة في تنفيذ هذه الجرائم،وأهم الركائز التي تعتمد عليها، وفي المبحث الثاني تناولنا كيفية تنفيذ عمليات النصب والاحتيال عبر مواقع التواصل الاجتماعي ، والعوامل التي تساعد على انتشار هذه الظاهرة مثل : سهولة الوصول للضحايا، ضعف الوعي الرقمي ،والثقة المفرطة وعرضنا إحصائيات ندعم فيها أبعاد الظاهرة وخطورتها.

<u>الفصل الثالث</u>: الهندسة الاجتماعية ودورها في وقوع الأفراد كضحايا للنصب والاحتيال

المبحث الأول: ماهية الهندسة الاجتماعية.

- تمهيد.

1- مفهوم الهندسة الاجتماعية.

2- فئات الهندسة الاجتماعية.

3- أمثلة عن الهندسة الاجتماعية.

4- أنواع الهندسة الاجتماعية.

المبحث الثاني:آليات وتداعيات الهندسة الاجتماعية في الاحتيال عبر مواقع التواصل .

1-أسباب انتشار الهندسة الاجتماعية .

2- مراحل الهجوم في الهندسة الاجتماعية.

3- وسائل الهندسة الاجتماعية.

4-النصائح التي يجي مراعاتها لتجنب الوقوع كضحية للهندسة الاجتماعية.

تمهيد:

مع التطور السريع للتكنولوجيا وانتشار الانترنت ، أصبحت مواقع التواصل الاجتماعي جزءا أساسيا من حياتنا اليومية ، حيث تستخدم للتواصل ، والتسوق ، ومشاركة المعلومات، ولكن مع هذا الانتشار الواسع ، ظهرت العديد من التحديات ، من بينها النصب والاحتيال الذي أصبح من أخطر التهديدات التي تواجه المستخدمين.

يعتمد المحتالون على الخداع والتلاعب النفسي لاستهداف الضحايا مستغلين ضعف الوعي الأمني ، أو الرغبة في الربح السريع. وتتنوع أساليبهم بين الرسائل المزيفة ، والعروض الوهمية، والروابط المشبوهة وانتحال الشخصيات ، كما يستغلون ثقة المستخدمين في المنصات الرقمية لاستدراجهم وسرقة أموالهم وبياناتهم الشخصية.

المبحث الأول: ماهية الهندسة الاجتماعية

الهندسة الاجتماعية منهجية تتيح للمهاجم تجاوز الضوابط التقنية عن طريق مهاجمة العنصر البشري في المؤسسة ،وذلك باستعمال مجموعة من الحيل النفسية لخداع الضحايا وإفشاء معلومات سرية وشخصية.

تستعمل الهندسة الاجتماعية غالبا دون الاعتماد على التقنيات ، بل بأساليب الخداع للحصول على المعلومات وتحصل الهندسة الاجتماعية عن طريق البريد الالكتروني أو انتحال شخصية ذات السلطة فمثلا، قد يتصل المهندس الاجتماعي بأحد الموظفين ويتظاهر بأنه من قسم تقانات المعلومات في الشركة ، في محاولة لخداع الموظف لإفشاء كلمة المرور الخاصة به.[1]

1/- مفهوم الهندسة الاجتماعية:

هي أسلوب تلاعب يستغل الخطأ البشري للحصول على معلومات خاصة أو الوصول إليها أو ممتلكات قيمة .في الجرائم الالكترونية غالبا،ما تغري عمليات الاحتيال " الاختراقية البشرية" هذه المستخدمين غير المنتبهين بكشف بياناتهم، أو نشر برمجيات خبيثة،أو منحهم إمكانية الوصول إلى أنظمة محظورة.يمكن أن تحدث الهجمات عبر الانترنت، أو وجها لوجه،أ وعبر تفاعلات أخرى.

تعتمد عمليات الاحتيال القائمة على الهندسة على طريقة تفكير الناس وتصرفاتهم ولذلك،تعد هجمات الهندسة الاجتماعية مفيدة بشكل خاص للتلاعب بسلوك المستخدم،يتمكن من خداعه والتلاعب به بفعالية بالإضافة إلى ذلك، يحاول المخترقون استغلال قلة معرفة المستخدم. وبفضل سرعة التكنولوجيا، يجهل العديد من المستهلكين والموظفين بعض التهديدات ، مثل:التنزيلات غير المقصودة.كما قد لا يدرك المستخدمون القيمة الكاملة للبيانات الشخصية ، مثل أرقام هواتفهم.ونتيجة لذلك ، يجهل العديد منهم

---

[1] _

http://scs.org.sy

كيفية حماية أنفسهم ومعلوماتهم على النحو بشكل عام، يكون لدى مهاجمي الهندسة الاجتماعية أحد هدفين:[1]

1/- التخريب: تعطيل أو إتلاف البيانات بهدف التسبب في ضرر أو إزعاج .

2/-السرقة: الحصول على أشياء ثمينة مثل:المعلومات أو الوصول أو الأموال.[2]

[1]-سعيد زيوش ،الاختراق عن طريق الهندسة الاجتماعية وأساليب الحماية منها،مجلة الاسرة والمجتمع،2021 ،ص175

[2]-http://www.kaspersky.com

2/-فئات الهندسة الاجتماعية:

الهندسة الاجتماعية وأولئك الذين يستخدمونها يمكن تقسيمهم إلى العديد من الفئات حيث نبدأ بمجموعة من الجواسيس والمتسللين حتى مندوبي المبيعات والأشخاص العاديين.

ا/- القراصنة (Rackers):

القراصنة يستفادون من الهندسة الاجتماعية مرات عديدة لأن عامل الضعف البشري هو أسهل بكثير في الاختراق من نقاط ضعف الشبكة. في مرات عديدة يفوز فيها القراصنة إذا كان الأمر يتعلق بمعركة يخوضها ضد مهندسي ومديري الشبكات وذلك لأنها ليست محدودة بسبب الوقت أو ضعف وجود الحافز .يعملون القراصنة 24 ساعة يوميا لإنجاز هدفهم .بعد أن يكونوا قد أمضوا الوقت وبذل العناية الواجبة للبحث في كل جانب من جوانب الهدف حتى يتمكنوا من شن هجوم شامل على البنية التحتية البشرية والتي يمكنها أن تدمر شركة في غضون دقائق. والحصول على المعلومات الشخصية .كلمة المرور، حسابات المستخدمين عن بعد والمزيد من القرصنة استخدام هذه المعلومات لتوجيه ضربة على الهدف.

ب/- الجواسيس أو التجسس (SpiesorEspionage):

الجواسيس من جميع أنحاء العالم تدرس أساليب مختلفة من " الخداع" لخداع ضحاياهم بالاعتقاد بأنهم شخص أو شيء آخر .بالإضافة إلى ذلك .يقومون بدراسة فن الهندسة الاجتماعية ، في مرات عديدة يقوم الجواسيس ببناء المصداقية من خلال المعرفة القليلة أو حتى الكثير عن العمل أو الحكومة التي يحاولون التجسس عليها.

ج/- لصوص الهوية (Indentitythieves):

سرقة الهوية هي استخدام المعلومات مثل: أسماء الأشخاص ،أرقام الحسابات المصرفية وعناوين وتواريخ الميلاد، ورقم الضمان الاجتماعي دون علم أصحابها هذا يمكن أن يترواح من وضع موحد لانتحال شخص ما ، أو عملية احتيال متقنة تشمل -DNS posoning) وحيل الخداع (phishing Scams) [1].

[1]-- الهاكر ألاخلاقي .ص791

د/- سماسرة المعلومات (Information Brokers):

سماسرة المعلومات (البيانات) يقومون بجمع البيانات وتقديم خدمات التنقيب عن البيانات للمنظمات المختلفة مثل مكتب التحقيقات الفيدرالي ،خدمات مراقبة الائتمان ، وزارة الدفاع، هذه الشركات هي ذات قيمة عالية بالنسبة للمهندسين الاجتماعيين لأنها تحتوي على كميات هائلة من المعلومات التي يمكن استخدامها لمزيد من رفع أو دعم أنشطة SE الخاص بك.

بسبب اللوائح والقوانين الفيدرالية فإن الكثير من المعلومات الشخصية التي يتم جمعها لدينا من قبل شركات سمسرة المعلومات كالأتي: Choicepoint –Kmawx– DOCUSEARcH – LexisnNexiS– DcxveetResarch– MasterFiles وغيرها من الشركات الأخرى .[1]

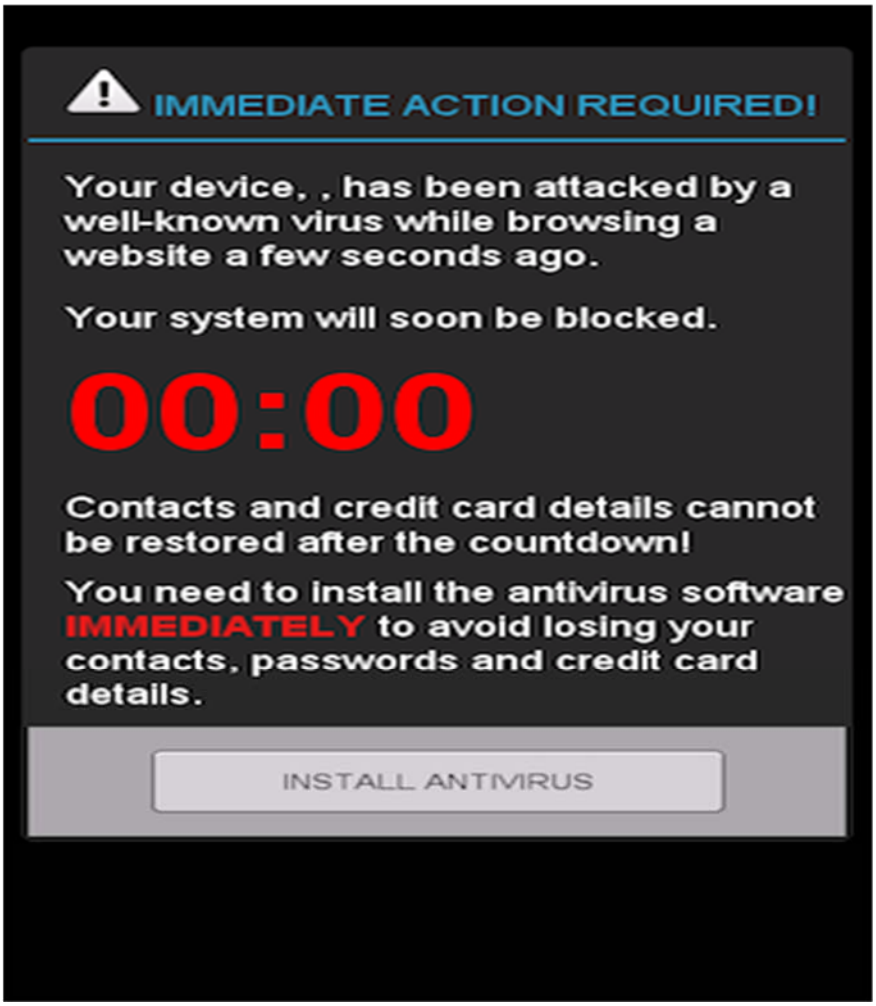
[1]- الهاكر ألاخلاقي .ص791

3/-أمثلة على الانتهاكات الناتجة عن الهندسة الاجتماعية:

أمثلة المحتوى المُخادِع:

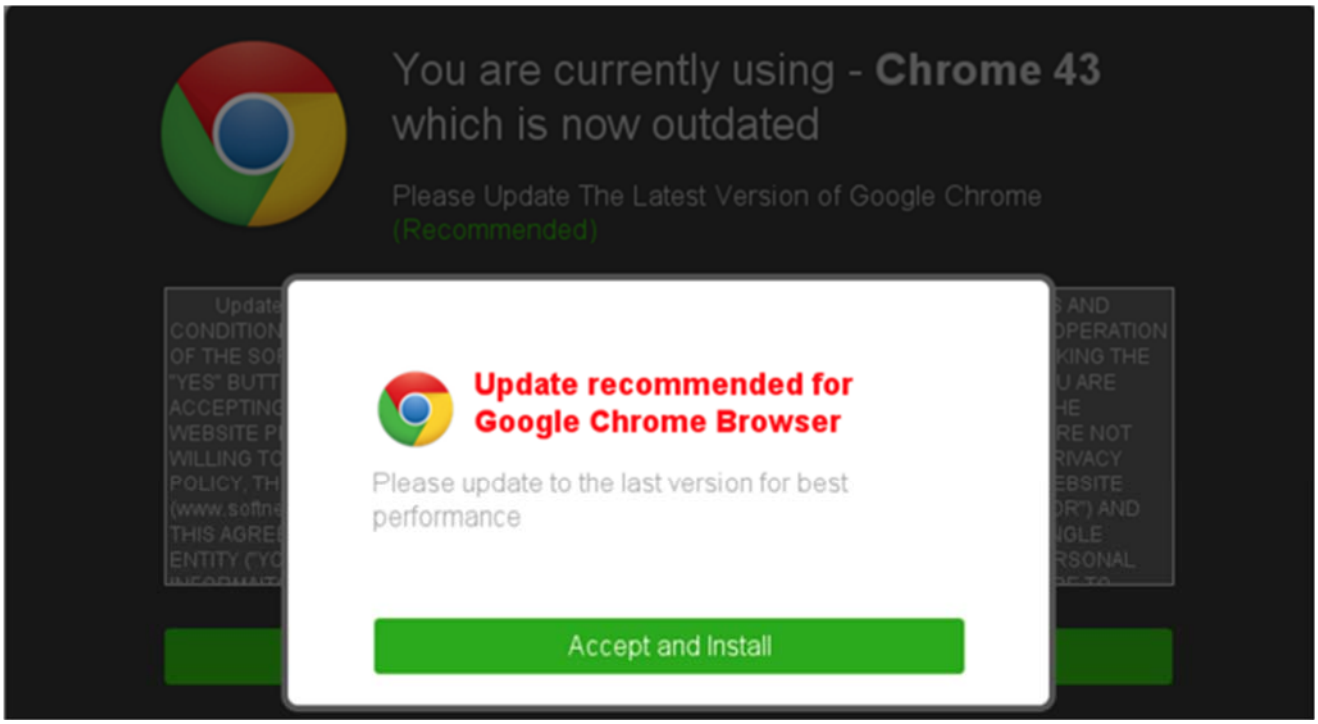
في ما يلي بعض الأمثلة على الصفحات التي تنخرط في ممارسات الهندسة الاجتماعي

نافذة منبثقة مخادعة تهدف إلى خداع المستخدم لحثّه على تثبيت برامج ضارة[1]



الشكل1: الصفحات التي تنخرط في ممارسات الهندسة الاجتماعي

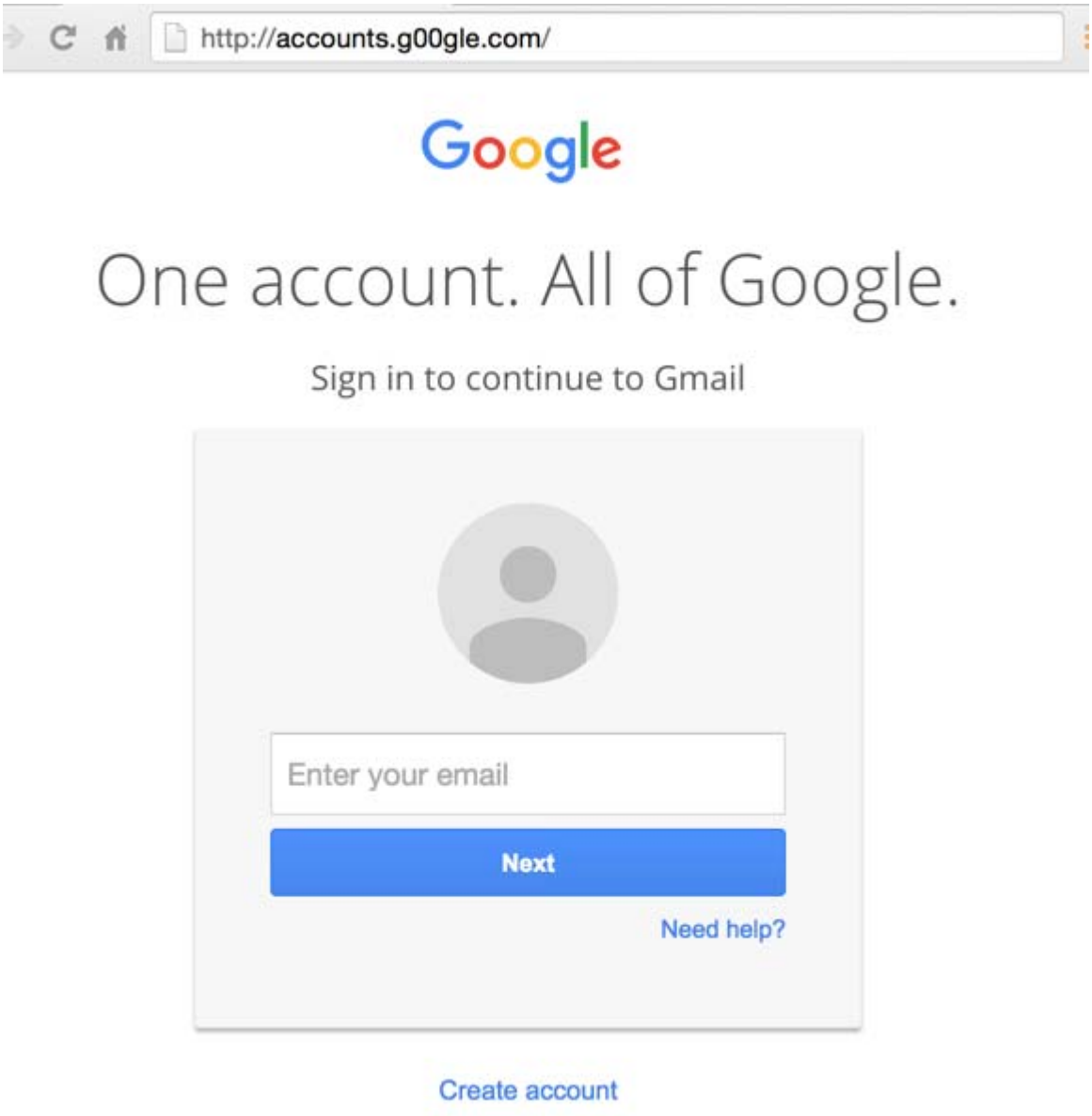
[1]-http://developers.google.com.



نافذة منبثقة مخادعة تدّعي مساعدة المستخدم في تحديث المتصفّح[1]

الشكل2: نافذة منبثقة مخادعة تدّعي مساعدة المستخدم في تحديث المتصفّح

[1]– http://developers.google.com

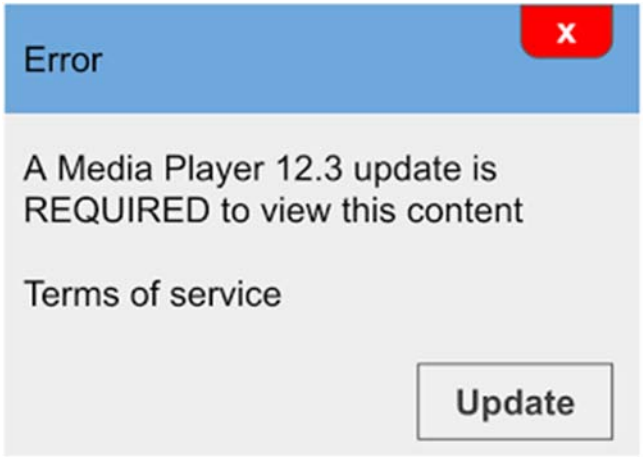


الشكل 3: صفحة مزيفة لتسجيل الدخول إلى Google

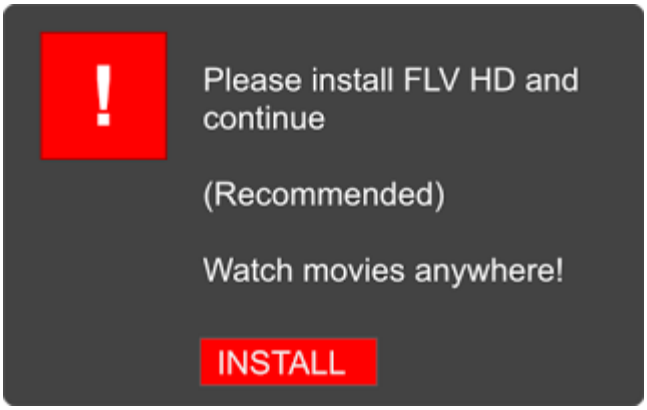
لاحِظ عنوان URL المخادع. قد تخدعك مواقع تصيّد احتيالي مشابهة أخرى بهدف حثّك على الإفصاح عن معلومات شخصية أخرى، مثل بيانات بطاقة الائتمان. قد تبدو مواقع التصيّد الاحتيالي بمظهر مطابق للموقع الإلكتروني الفعلي، لذا تأكّد من الاطّلاع على شريط العنوان للتحقق من صحة عنوانURL ، وتحقَّق أيضًا من أنّ عنوان الموقع الإلكتروني يتضمّن البادئة.**https://**

أمثلة على الإعلانات المخادعفي ما يلي بعض الأمثلة على المحتوى المخادع في الإعلانات المضمَّنة. تظهر هذه الإعلانات كجزء من واجهة الصفحة وليس باعتبارها إعلانات[1].

[1] http://developers.google.com



الشكل 4: نافذة منبثقة مخادعة تدّعي أنّ أحد البرامج المثبّتة على جهاز المستخدم قديم



الشكل 5: نافذة منبثقة مخادعة تدعي أنّ مصدرها مطوّر FLV



إعلانات تتنكّر في شكل أزرار الإجراءات على الصفحة[1]

[1]- http://developers.google.com

4/ أنواع الهندسة الاجتماعية:

في هجوم الهندسة الاجتماعية، يستخدم المهاجم المهارات الاجتماعية للتحايل على الضحية بغرض كشف معلومات شخصية مثل أرقام بطاقات الائتمان وأرقام الحسابات المصرفية وأرقام الهاتف، أو معلومات سرية عن منظمتهم أو نظام الكمبيوتر، وذلك باستخدامهم إما لإطلاق الهجوم أو الاحتيال.يمكن تقسيم الهندسة الاجتماعية على نطاق واسع إلى ثلاثة أنواع: استنادا إلى الإنسان.استنادا إلى الحاسوب.استنادا إلىmobile.

أ/- هجمات الهندسة الاجتماعية المستندة إلى الإنسان:

الهندسة الاجتماعية القائمة على الإنسان تنطوي على التفاعل مع الإنسان بطريقة أو بأخرى.من خلال التفاعل مع الضحية.المهاجم يجمع المعلومات المطلوبة عن المنظمة. على سبيل المثال: عن طريق انتحال شخصية It للدعم الفني، يمكن للمهاجم الحصول على الوصول بسهولة إلى غرفة الخادم. وفيما يلي الطرق التي يمكن أن تؤدي هجوم الهندسة الاجتماعية القائمة على الإنسان:

- التظاهر بأنه المستخدم النهائي للمشروع.
- التظاهر بأنه مستخدم هام.
- متنكرين في زي الدعم الفني.

ب/- هجمات الهندسة الاجتماعية على الحاسوب:

الهندسة الاجتماعية المستندة إلى الحاسوب تعتمد على أجهزة الكمبيوتر وأنظمة الانترنت لتنفيذ الإجراء المستهدف ، وفيما يلي الطرق التي يمكن أن يؤدي المهاجم الهندسة الاجتماعية المعتمدة على الكمبيوتر:

- التصيد (phishing).
- البريد الوهمي .
- هجمات النافذة المنبثقة (pop-up windowattacks).[1]

ج/- هجمات الهندسة الاجتماعية المستندة على الهاتف الجوال:

[1]- الهاكر الأخلاقي .نفس المرجع .ص 806.

تتم عن طريق المساعدة من تطبيقات الجوال. المهاجمين يقومون بإنشاء تطبيقات خبيثة مع مميزات جذابة وأسماء مشابهة لتلك التطبيقات الشعبية، ونشرها في المتاجر الكبرى للتطبيق.عندما يقوم المستخدم بتحميل هذه التطبيقات فإنه يتم مهاجمته من قبل البرمجات الخبيثة.وفيما يلي الطرق التي يمكن أن تؤدي هجوم الهندسة الاجتماعية على المحمول:

- نشر التطبيقات الخبيثة.
- إعادة تحريم التطبيقات الشرعية.
- تطبيقات الأمن الوهمية باستخدام رسائل SMS .[1]

[1]–الهاكر الأخلاقي .نفس المرجع .ص 806.

المبحث الثاني: آليات وتداعيات الهندسة الاجتماعية في الاحتيال عبر مواقع التواصل.

1/أسباب انتشار الهندسة الاجتماعية:

- الافتقار إلى وضع سياسات تحمي النظام ومستخدمي النظام .
- سهولة الوصول لأية معلومة وخاصة مع انتشار الشبكات الاجتماعية ومحركات البحث.
- قلة التدريب في المجال الأمني للمعلومات.
- تقسيم المؤسسة أو الدولة إلى وحدات منفصلة.
- سهولتها مقارنة بالوسائل التقنية الأخرى ، حيث يمكن تحقيقها بمجرد انتهاك العلاقات الإنسانية وقد لا تتطلب خبرة كبيرة من الناحية التقنية
- المعدات الأمنية والتقنية لا تمنع من وقوعها لأنها ترتكز على الجانب الإنساني.
- المهاجم لا يحتاج معدات أو مهارات متخصصة .فهي أسلوب غير مكلف.
- كتمان الضحايا للأخطاء والسرقات التي تحدث لهم.
- عدم إدراك أهميتها ومدى خطورتها من قبل المتخصصين في مجال أمن المعلومات وكذلك مستخدمي الحاسوب.
- صعوبة الكشف عنها وتتتبع أثرها.[1]

[1]–اضاءات الهندسة الاجتماعية : السلسلة 11 .العدد 4. نشرة توعوية يصدرها معهد الدراسات المصرفية .دولة الكويت – مارس 2019 ص4.

2/- مراحل الهجوم في الهندسة الاجتماعية:

المهاجم ينفذ الهندسة الاجتماعية في التسلسل التالي:

أ/- البحث عن الشركة المستهدفة:

المهاجم قبل مهاجمة أي شبكة في الواقع ، يجمع المعلومات من أجل إيجاد السبل الممكنة لدخول الشبكة المستهدفة .الهندسة الاجتماعية هي واحدة مثل هذه التقنية لانتزاع المعلومات –المهاجم يقوم في البداية بأبحاث على الشركة المستهدفة للعثور على المعلومات الأساسية مثل نوع الأعمال ،موقع المنظمة ،عدد الموظفين وما إلى ذلك وخلال هذه المرحلة، المهاجم قد يجري البحث في القمامة ،تصفح موقع الشركة ،العثور على تفاصيل الموظف.

ب/- تحديد الضحية :

بعد إجراء بحوث متعمقة عن الشركة المستهدفة، المهاجم يختار الضحية الرئيسية لمحاولة استغلالها للاستيلاء على المعلومات الحساسة والمفيدة. الموظفين الساخطين للشركة هي أكبر فرصة للمهاجم .المهاجم يحاول أن يجد هؤلاء الموظفين واستدراجهم للكشف عن معلومات الشركة .حيث أنهم غير راضيين عن الشركة ،فإنهم قد يكونا على استعداد لتسريب أو الكشف عن البيانات الحساسة للشركة إلى المهاجم.

ج/- استغلال العلاقة:

بمجرد قيام المهاجم ببناء علاقة مع العاملين في الشركة ، فإنه يحاول استغلال العلاقة مع موظفي الشركة ويحاول استخراج معلومات حساسة مثل معلومات الحساب ،والمعلومات المالية ،والتكنولوجيات الحالية المستخدمة ، وخطط المستقبل.[1]

[1]-- الهاكر الاخلاقي : مرجع سابق ص794- 795.

د/- تطوير العلاقة:

بمجرد أن يتم تحديد هؤلاء الموظفين فإن المهاجمين يدخلون في محاولة لتطوير العلاقات معهم حتى يتمكنوا من استخراج المعلومات السرية منها بعد ذلك يقوموا بالاستخدام هذه المعلومات لاستخراج المزيد من المعلومات أو لشن الهجمات.[1]

3/- وسائل الهندسة الاجتماعية:

تنوعت الوسائل التقنية لتشمل ما يلي:

أ/- التصيد:

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء كانت معلومات شخصية أومالية عن طريق رسائل البريد الالكترونية أو مواقع الانترنت التي تبدو كأنها مبعوثة من شركات موثوقة أو مؤسسات مالية أو حكومية . من أجل توصيل رسالة التصيد التي ستقنع الضحية إما بإفصاح المباشر عن المعلومات أو القيام بإجراء (مثل الدخول إلى موقع وهمي على شبكة الانترنت أو النقر فوق رابط تحميل لأحد البرامج الخبيثة). يسمح للمهاجم – دون علم الضحية – بالاستمرار في خطة ذات النية السيئة.

يمكن الانتباه من التصيد من خلال الإرشادات التالية :

- حماية جهاز الحاسوب باستخدام برامج مضاد الفيروسات (anti-virures) وجدار النار (firewalls) كما يجب تحديثها باستمرار.
- تنزيل شريط أدوات لمتصفح الانترنت للحماية من المواقع الالكترونية المزيفة المعروفة.
- يجب عدم الوثوق بأي رابط وإن كان مرسلا من أحد أصدقائك.
- لاتدخل معلوماتك في أي موقع بشكل عشوائي ودون التأكد من اسم الموقع وصحته.
- التأكد بأن بداية عنوان الموقع في شريط العنوان المتصفح هو https//: فوجود حرف (s) يعني موقع آمن من خلال استخدام تقنية التشفير . بالإضافة إلى أن الصفحة تتضمن توقيع رقمي (digital sign) وبغيرهما معا يصعب التأكد والوثوق بالصفحة.

[1]- الهاكر الاخلاقي : مرجع سابق ص794- 795.

- تجنب تعبئة النماذج المتعلقة بالمعلومات المالية أو التي تطلب أية معلومات في الرسائل الالكترونية. [1]

ب/- الشبكات الاجتماعية:

- يجب معرفة أن معظم الحسابات الاجتماعية تكون مكشوفة للشركات المالكة له ولديه الحق في نقلها لطرف آخر أو نشرها .[2]
- إن تطبيق الفيسبوك هو أكثر عرضة لهجمات الهندسة الاجتماعية وذلك لتوفر كم كبير من البيانات الشخصية .كما يعاني مستخدمي الفيسبوك غالبا من هجمات الفيروسات، حيث يعتبر وسيلة سهلة لنقل الفيروسات من خلال الصور وغيرها من عناصر متاحة.
- يكون الشخص معرض لاختراق من ناحيتين : الشركة التي تكون مطلعة على جميع بياناتك بالإضافة إلى الصلاحيات التي تسلبها منك .وكذلك اختراق الأفراد والتي قد يحدث بأكثر من طريقة.
- يقوم المهندس الاجتماعي باستغلال البيانات الموجودة في الشبكات خاصة في الشبكات الاجتماعية مهما كانت بسيطة.
- يجب عدم الثقة بالمعلومات أو الأشخاص في الشبكات الاجتماعية ، قد يكونوا الطعم لعملية احتيال جديدة.

ت/- الهواتف:

تعد الهواتف أحد أساليب الهندسة الاجتماعية المستخدمة بكثرة في الوقت الحاضر وتتضمن نوعين هما:

- مكالمات صوتية وتسمى(Vishing) :وهي أن تأتيك مكالمة صوتية تدعي أنك فائز بجائزة نقدية كبيرة مثلا أو أن يعرقك ليقوم بالاحتيال عليك.

[1]- ا لهندسة الاجتماعية، نشرة توعوية يصدرها معهد الدراسات المصرفية .دولة الكويت- مارس 2019. السلسلة 11-العدد4.ص 5.

- مكالمات نصية وتسمى (Smishing) : وهي أن تصل إليك رسالة نصية تثير عندك الفضول أو الطمع ليجبرك أن تقوم بالضغط على رابط يؤدي إلى اختراق جهازك.

د/- البرمجيات الخبيثة:

يمكن العثور على العديد من عينات البرامج الخبيثة المثيرة لاهتمام والتي تعتمد على الهندسة الاجتماعية من أجل توصيل هجومها إلى الضحية بشكل فعال.ومن أشهر الوسائل المستخدمة في عملية التوصيل هو ما يسمى بالتحديات الوهمية لبرنامج flash player والملفات المدمجة في وثائق وورد ، ونسخ المتصفحات المشروعة ذات الجودة المنخفضة مثل انترنت اكس بلور وغيرها .[1]

4/- النصائح التي يجب مراعاتها:

- لا تثق بأي ر مكالمة هاتفية أو بريد الكتروني من أي شخص يطلب منك معلومات شخصية أو بنكية ويجب التأكد من هوية هذا الشخص عن طريق الاتصال بالمصدر للتحقق من هوية طالب المعلومات.
- تجنب استخدام البطاقة الائتمانية إلا عند الضرورة القصوى واستخدام البطاقات مسبقة الدفع عوضا عن ذلك.
- تجنب وضع المعلومات الشخصية على الانترنت مثل الاسم واللقب ورقم الجوال وأي معلومات بنكية.
- التأكيد على ضرورة إتلاف الأوراق والمستندات المهمة بواسطة أجهزة مخصصة لهذا الغرض.
- تجنب كل الرسائل الالكترونية التي تحتوي على روابط مشبوهة في البريد -الالكتروني أو رسائل الجوال أو على المواقع الاجتماعية.[2]

[1]- الهندسة الاجتماعية، نشرة توعوية يصدرها معهد الدراسات المصرفية .دولة الكويت- مارس 2019. السلسلة 11-العدد4.ص-7.

[2]- م. مها أحمد إبراهيم محمد :الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات- مج5، ع3 (يوليو -سبتمبر 2018) ص 119.

الخاتمة:

تناولنا في هذا الفصل على مبحثين، تطرقنا في المبحث الأول على مفهوم الهندسة الاجتماعية باعتبارها أسلوبا يستخدمه المحتالون لخداع الضحايا واستغلالهم نفسيا واجتماعيا للحصول على معلومات حساسة أو تحقيق مكاسب غير مشروعة.بدأنا بتوضيح ماهية الهندسة الاجتماعية وأهدافها ،ثم انتقلنا إلى شرح مراحل الهجوم باستخدام هذا الأسلوب مثل: الاستدراج، بناء الثقة،،ثم الاستغلال، كما تناولنا الوسائل والأساليب التي تعتمدها الهندسة الاجتماعي .وفي المبحث الثاني بينا دور العوامل النفسية والاجتماعية التي تجعل الأفراد عرضة لهذا النوع من الاحتيال وفي الختام قدمنا توصيات تساعد للحد من تأثير هذه الممارسات عبر تعزيز الوعي الرقمي والأمني.

الفصل الرابع : الجانب التطبيقي

المبحث الأول : البيانات العامة

1/خصائص عينة الدراسة:

من أجل معرفة خصائص العينة المدروسة، تم الإعتماد على إستجابات أفرادها فيما يخص الجزء الأول (بيانات العامة) للعينة المدروسة من الإستمارة، وهو ما سنوضحه فيما يلي:

أ/ توزيع عينة الدراسة وفقا للجنس:

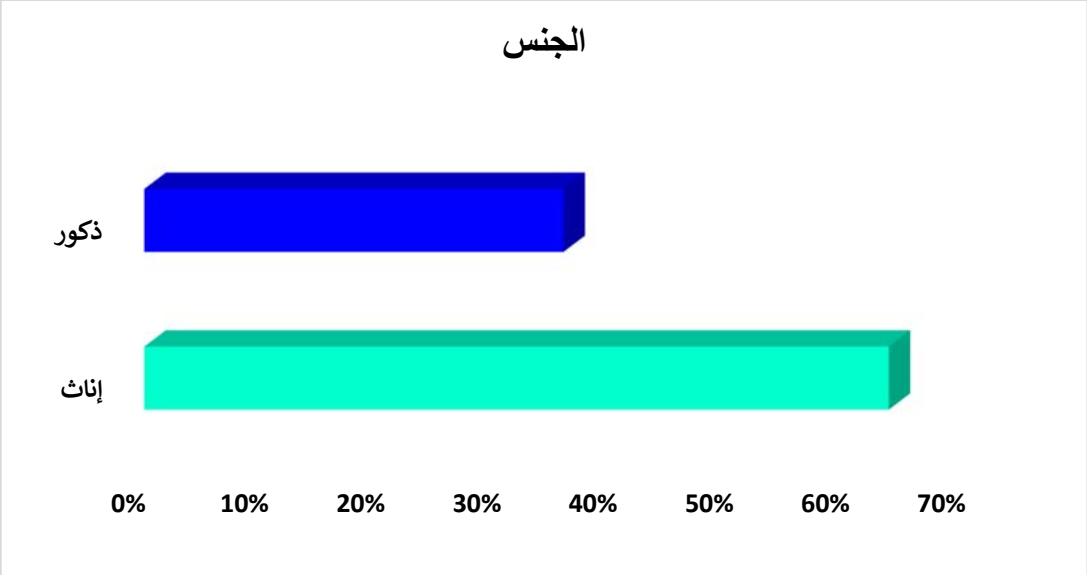
من خلال الجدول الموالي والشكل البياني أسفله يتم التعرف على توزيع مفردات العينة وفقا لمتغير الجنس (ذكر، أنثى)، والتي توزعت كما يلي:

الجدول 4: توزيع عينة الدراسة حسب الجنس

المتغير	الفئة	التكرار	النسبة المئوية
الجنس	ذكور	27	%36
	إناث	49	%64
	المجموع	76	%100

يتضح لنا من خلال الجدول أعلاه أن عدد أفراد العينة من الذكور بلغ: 27 فردا بما نسبته: 36%، في حين أن عدد الإناث المستجوبات قدر بـ: 49 فرد بنسبة تقدر بـ: 64%، وهذه النتيجة تدل على تنوع عينة الدراسة من حيث الجنس.

والشكل الموالي يوضح هذه النسب بين الجنسين:



الشكل 6: توزيع عينة الدراسة حسب الجنس

ب/ توزيع عينة الدراسة وفقا للسن:

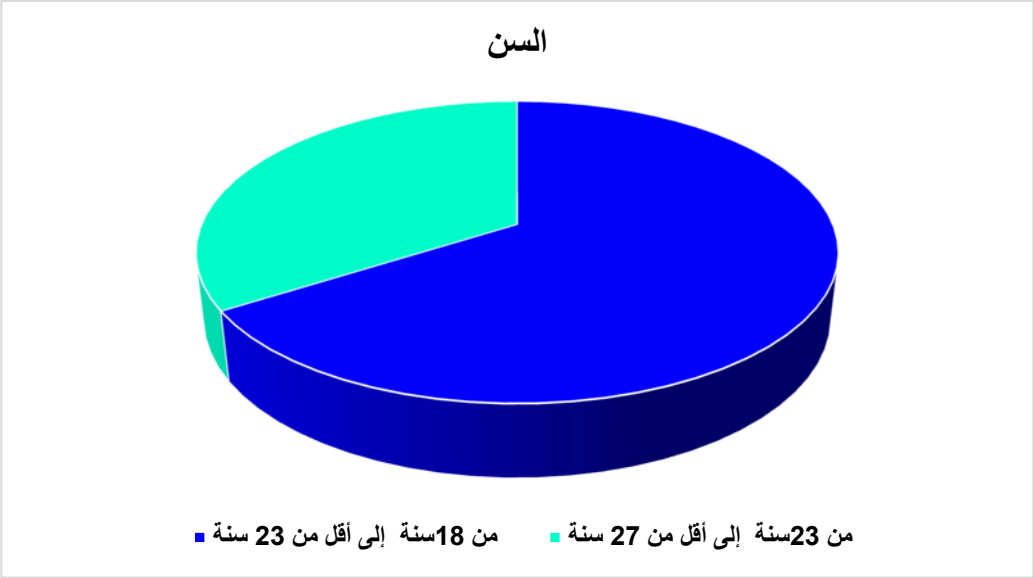
من خلال الجدول الموالي والشكل البياني أسفله يتم التعرف على توزيع مفردات العينة وفقا لمتغير السن، والتي كانت على النحو التالي:

الجدول 5: توزيع عينة الدراسة حسب السن

المتغير	الفئة	التكرار	النسبة المئوية
السن	من 18سنة إلى أقل من 23 سنة	50	%66
	من 23سنة إلى أقل من 27 سنة	26	%34
	المجموع	76	%100

يتضح لنا من خلال الجدول أعلاه والخاص بتوزيع مفردات عينة الدراسة وفقا لمتغير السن أن الفئة العمرية (من 18 سنة إلى أقل من 23 سنة) هي الفئة الأكثر تواجدا في التوزيع حيث قدر عددها بـ: 50 فرد بنسبة: 66%، في مقابل 26 فردا للفئة العمرية (من 23 سنة إلى أقل من 27 سنة) بنسبة: 34%، وهذه النتيجة تدل على تنوع أفراد العينة من حيث العمر، إذ أن الدراسة تستهدف مختلف الفئات العمرية.

والشكل الموالي يوضح تباين هذه النسب حسب السن:



الشكل 7: توزيع عينة الدراسة حسب السن

ج/ توزيع عينة الدراسة وفق المستوى الدراسي:

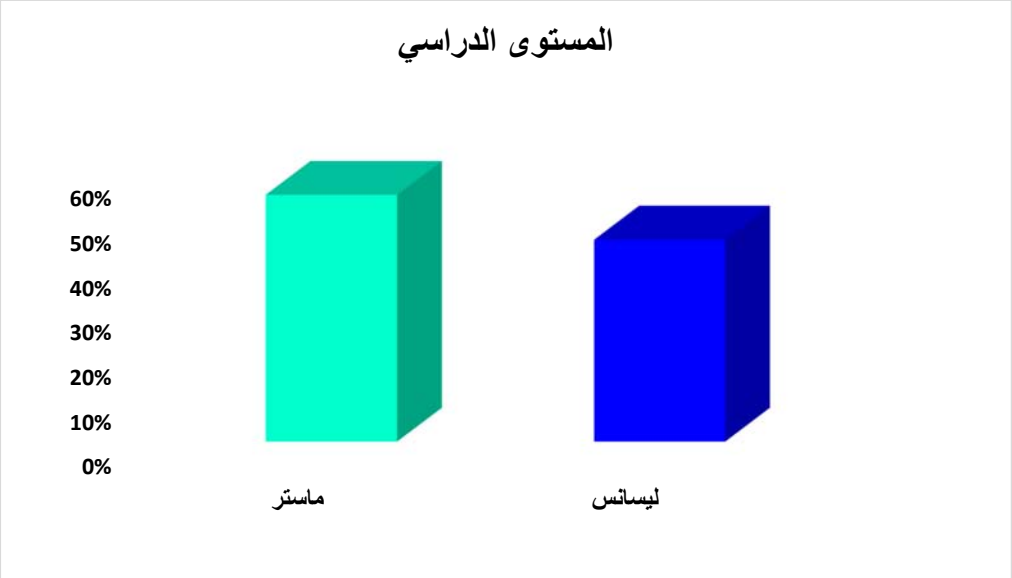
من خلال الجدول الموالي والشكل البياني أسفله يتم التعرف على توزيع مفردات العينة وفقا لمتغير المستوى الدراسي، والتي جاءت على النحو التالي:

الجدول 6: توزيع عينة الدراسة حسب المستوى الدراسي

المتغير	المستوى	التكرار	النسبة المئوية
المستوى الدراسي	ليسانس	34	%45
	ماستر	42	%55
	المجموع	76	%100

يتضح لنا من خلال الجدول أعلاه والخاص بتوزيع مفردات عينة الدراسة وفقا لمتغير المستوى الدراسي أن طلبة الماستر هي الفئة الأكثر تواجدا في التوزيع حيث قدر عددها بـ: 42 فرد بنسبة: 55%، في مقابل 34 فردا لطلبة الليسانس بنسبة: 45%، وهذه النتيجة تدل على تنوع أفراد العينة من حيث المستوى الدراسي.

والشكل الموالي يوضح تباين هذه النسب فيما يخص المستوى الدراسي:



الشكل 8: توزيع عينة الدراسة حسب المستوى الدراسي

د/ توزيع عينة الدراسة وفقا للإقامة:

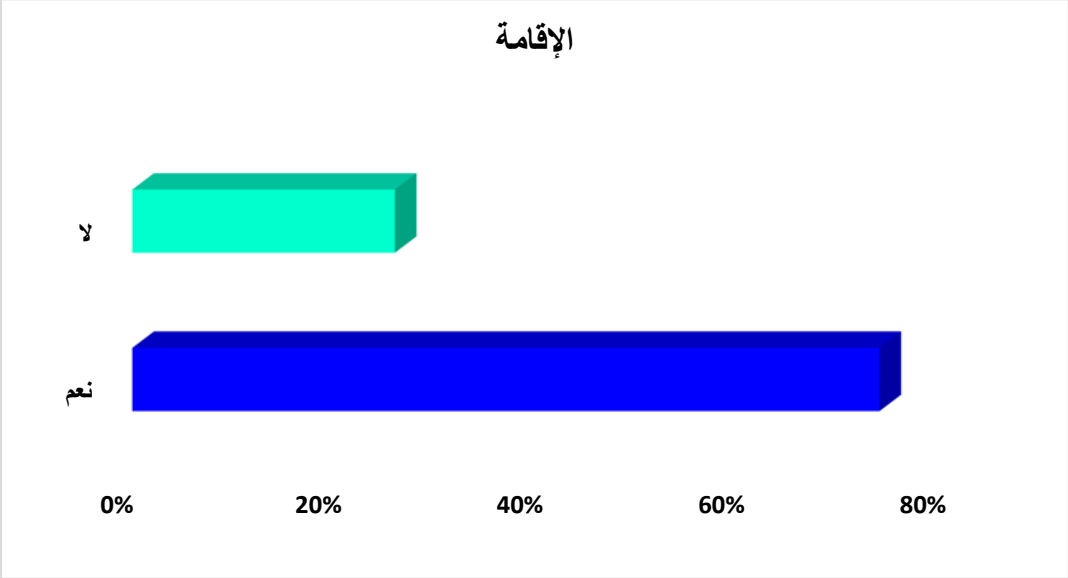
من خلال الجدول الموالي والشكل البياني أسفله يتم التعرف على توزيع مفردات العينة وفقا لمتغير الإقامة، والتي توزعت على النحو التالي:

الجدول 7: توزيع عينة الدراسة حسب الإقامة

المتغير	المستوى	التكرار	النسبة المئوية
الإقامة	لا	20	%26
	نعم	56	%74
	المجموع	76	%100

يتضح لنا من خلال الجدول أعلاه والخاص بتوزيع مفردات عينة الدراسة وفقا لمتغير الإقامة أن غالبية الطلبة في العينة من المقيمين، حيث قدر عددهم بـ: 56 فردا بنسبة: 74%، في مقابل 20 فردا من الطلبة غير المقيمين بنسبة: 26%.

والشكل الموالي يوضح تباين هذه النسب فيما يخص الإقامة:



الشكل 9: توزيع عينة الدراسة حسب الإقامة

هـ/ توزيع عينة الدراسة وفقا للتخصص:

من خلال الجدول الموالي والشكل البياني أسفله يتم التعرف على توزيع مفردات العينة وفقا لمتغير التخصص في الجامعة، والتي جاءت على النحو التالي:

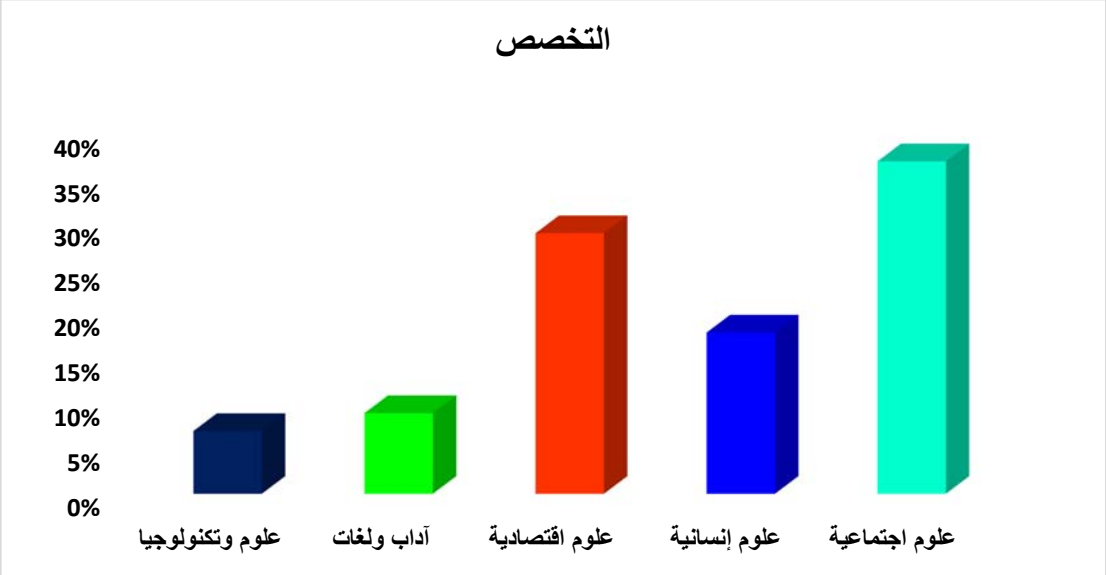
الجدول 8: توزيع عينة الدراسة حسب التخصص

المتغير	الفئة	التكرار	النسبة المئوية
التخصص	علوم اجتماعية	28	%37
	علوم إنسانية	14	%18
	علوم اقتصادية	22	%29
	آداب ولغات	7	%9

	علوم وتكنولوجيا	5	%7
	المجموع	76	%100

يتضح لنا من خلال الجدول أعلاه والخاص بتوزيع مفردات عينة الدراسة وفقا لمتغير التخصص أن طلبة العلوم الاجتماعية هم الفئة الأكثر ظهورا في العينة بواقع 28 فردا أي ما نسبته: 37%، يليها تخصص العلوم الاقتصادية بواقع 22 فردا أي ما نسبته: 29%، ثم تخصص العلوم الإنسانية بواقع 14 فردا أي ما نسبته: 19%، بينما قدر عدد طلبة الآداب واللغات الأجنبية بـ: 7 أفراد بنسبة تقدر بـ: 9%، في حين أن فئة طلبة تخصص العلوم والتكنولوجيا جاءت في المرتبة الأخيرة من حيث العدد والبالغ: 5 أفراد بنسبة: 7%.

والشكل الموالي يوضح تباين هذه النسب بين فئات عينة الدراسة حسب التخصص:



الشكل 10: توزيع عينة الدراسة حسب التخصص

عرض نتائج محور عادات استخدام مواقع التواصل الاجتماعي:

1. يؤثر متغير الإقامة بالأحياء الجامعية على مدى استخدام مواقع التواصل الاجتماعي.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (χ^2 كا) للاستقلالية، لتحديد ما إذا كانت الإقامة في الأحياء الجامعية تؤثر على مدى استخدام الطالب لمواقع التواصل الاجتماعي أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 9: اختبار (كا2) للاستقلالية لتحديد الفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للإقامة في الأحياء الجامعية

مدة الاستخدام	الإقامة				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	مقيم		غير مقيم						
	F	%	F	%	F	%			
يوميا	14	70	55	98	69	90	11.78	0.008	دال إحصائيا
أسبوعيا	2	10	0	0	2	3			
شهريا	2	10	0	0	2	3			
نادرا	2	10	1	2	3	4			
المجموع	21	100	56	100	76	100			

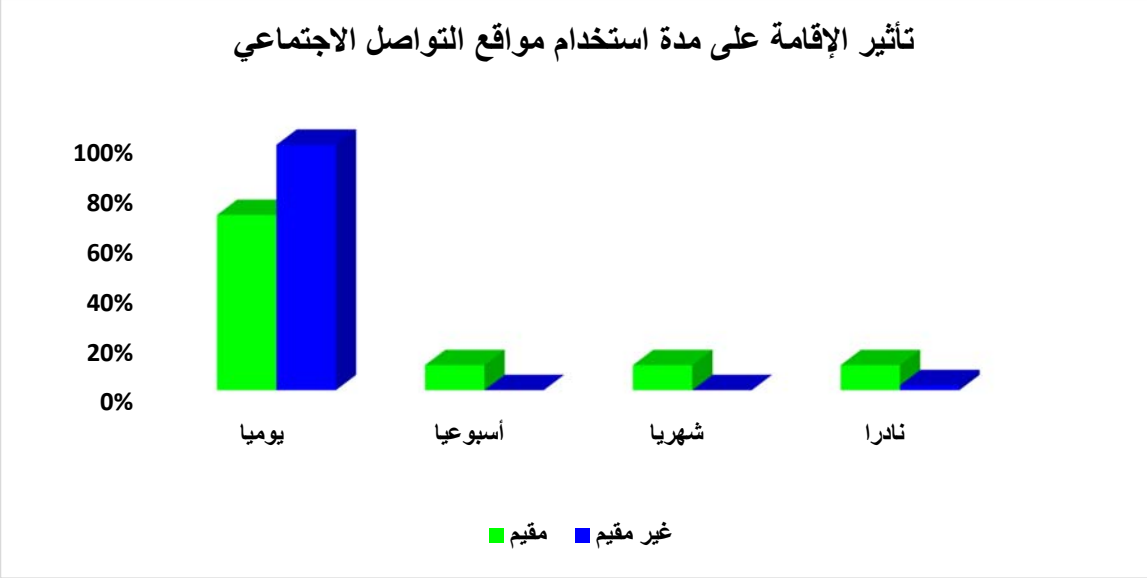
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الطلبة المقيمين: نجد أن 70% منهم يستخدمون مواقع التواصل الاجتماعي بشكل يومي، يليها المستخدمون للمواقع بشكل أسبوعي أو شهري أو نادرا بنسبة: 10% لكل منها.

أما بالنسبة لفئة الطلبة غير المقيمين: فنجد أن جلهم 98% يستخدمون مواقع التواصل الاجتماعي بشكل يومي، فيما 2% فقط نادرا ما يستخدمون مواقع التواصل، مع تسجيل غياب تام في هذه الفئة لمن يستخدمون المواقع بشكل أسبوعي أو شهري.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(11.78)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α= 0.01)** ودرجة حرية **(df= 3)**، وعلى هذا الأساس يمكن القول أن متغير الإقامة يؤثر في مدة استخدام الطلبة الجامعيين لمواقع التواصل الاجتماعي.

والشكل الموالي يوضح الأمر أكثر.



الشكل 11: أعمدة بيانية للفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للإقامة في الأحياء الجامعية

2. يؤثر متغير السن في مدة استخدام مواقع التواصل الاجتماعي.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كان سن الطالب الجامعي يؤثر على مدة استخدامه لمواقع التواصل الاجتماعي أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 10: اختبار (كا2) للاستقلالية لتحديد الفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للسن

مدة الاستخدام	السن				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	من 18 سنة إلى أقل من 23 سنة		من 23 سنة إلى أقل من 27 سنة						
	F	%	F	%	F	%			
أقل من ساعة	2	4	5	19	07	10	6.88	0.075	غير دال إحصائيا
من ساعة إلى 3 ساعات	23	46	6	24	29	38			
من 3 إلى 5 ساعات	9	18	5	19	14	18			
أكثر من 5	16	32	10	38	26	34			

ساعات							
المجموع	50	100	26	100	76	100	

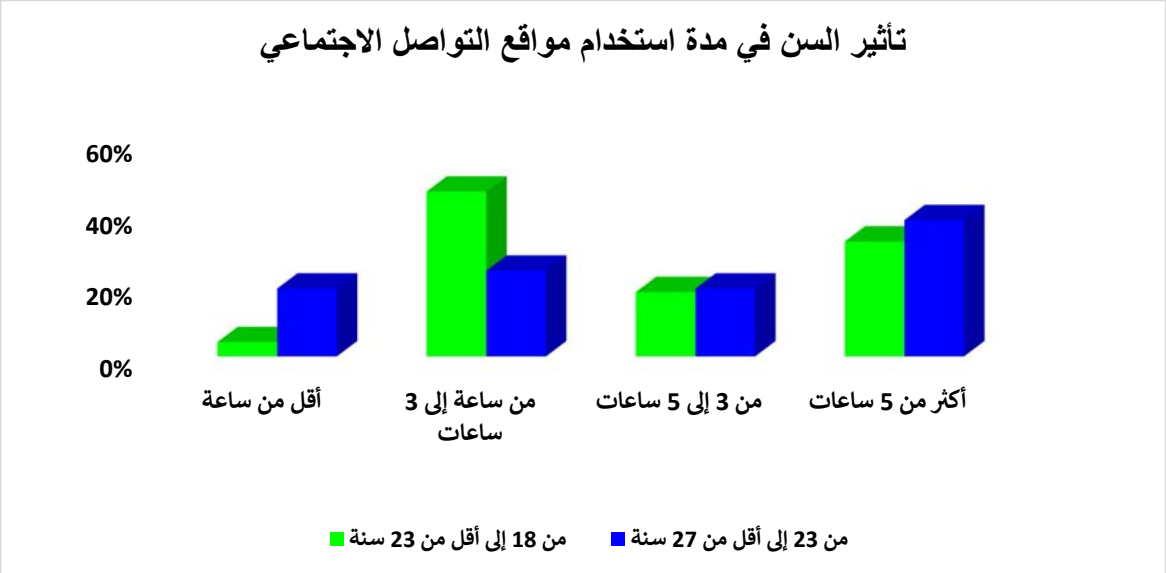
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة للفئة العمرية من 18 إلى أقل من 23 سنة: نجد أن 46% منهم يستخدمون مواقع التواصل الاجتماعي ما بين 1 ساعة إلى 3 ساعات يوميا، يليها المستخدمون للمواقع لأكثر من 5 ساعات بنسبة تقدر بـ: 32%، ثم المستخدمون لمواقع التواصل الاجتماعي لمدة من 3 إلى 5 ساعات بنسبة: 18%، وأخيرا المستخدمون للمواقع لأقل من 1 ساعة واحدة بنسبة: 4%.

أما بالنسبة للفئة العمرية من 23 إلى أقل من 27 سنة: نجد أن 38% منهم يستخدمون مواقع التواصل الاجتماعي لأكثر من 5 ساعات يوميا، يليها المستخدمون للمواقع ما بين 1 ساعة واحدة و3 ساعات بنسبة تقدر بـ: 24%، فيما جاءت أخيرا فئة المستخدمين لأقل من 1 ساعة وفئة المستخدمين من 3 إلى 5 ساعات مناصفة بينهما بواقع 19%.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(6.88)** وهي قيمة غير دالة إحصائيا، وعلى هذا الأساس يمكن القول أن متغير السن لا يؤثر في مدة استخدام الطلبة الجامعيين لمواقع التواصل الاجتماعي.

والشكل الموالي يوضح الأمر أكثر.



الشكل 12: أعمدة بيانية للفروق في مدة استخدام الطالب لمواقع التواصل الاجتماعي تبعا للسن

3. يؤثر متغير الجنس في موقع التواصل الاجتماعي المستخدم من طرف الطالب الجامعي.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كان جنس الطالب الجامعي يؤثر على طبيعة مواقع التواصل الاجتماعي الأكثر استخداما أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 11: اختبار (كا2) للاستقلالية لتحديد الفروق في أكثر مواقع التواصل الاجتماعي استخداما تبعا للجنس

مواقع التواصل	الجنس				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	ذكر		أنثى						
	F	%	F	%	F	%			
تيك توك	8	30	8	16	16	21	7.06	0.21	غير دال إحصائيا
فايسبوك	7	25	22	45	29	38			
انستغرام	7	25	13	27	20	26			
تيليغرام	2	8	0	0	2	3			
سناب شات	1	4	1	2	2	3			
واتساب	2	8	5	10	7	9			
المجموع	27	100	49	64	76	100			

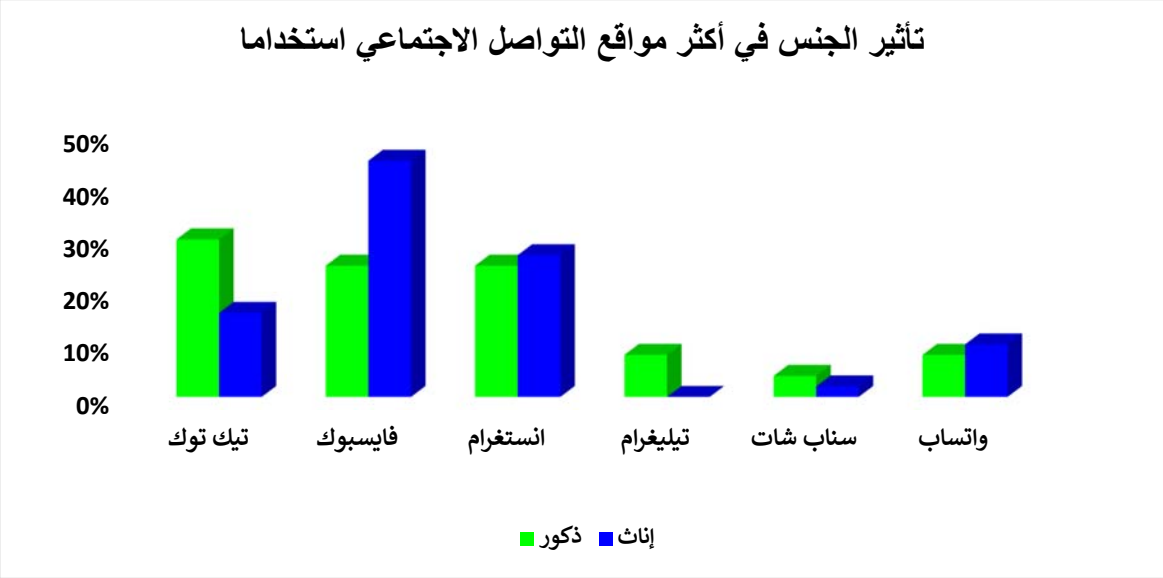
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الذكور: نجد أن 30% منهم يستخدمون تيك توك، يليها المستخدمون لموقعي فايسبوك وانستغرام مناصفة بينهما بنسبة 25%، ثم المستخدمون لموقعي تيليغرام وواتساب مناصفة بينهما بنسبة: 8%، وأخيرا المستخدمون لموقع سناب شات بنسبة: 4%.

أما بالنسبة لفئة الإناث: نجد أن 45% منهن يستخدمن موقع فايسبوك، يليها المستخدمات لموقع وانستغرام بنسبة 27%، ثم المستخدمات لموقع تيك توك بنسبة: 16%، يليها المستخدمات لموقع واتساب بنسبة 10%، وأخيرا المستخدمات لموقع سناب شات بنسبة: 2%، مع تسجيل غياب تام للمستخدمات لموقع تيليغرام.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(7.06)** وهي قيمة غير دالة إحصائيا، وعلى هذا الأساس يمكن القول أن متغير الجنس لا يؤثر في موقع التواصل الاجتماعي الاجتماعي الأكثر استخداما من قبل الطالب الجامعي.

والشكل الموالي يوضح الأمر أكثر.



الشكل 13: أعمدة بيانية للفروق في في أكثر مواقع التواصل الاجتماعي استخداما تبعا للجنس

2/ عرض نتائج محور الأمن السبراني:

1. يؤثر متغير المستوى الدراسي في استخدام كلمات قوية وفريدة.

وللتحقق من صحة هذا الطرح تم اللجوء إلى اختبار **(كا^2)** χ للاستقلالية، لتحديد ما إذا كان المستوى الدراسي للطالب الجامعي يؤثر على قوة كلمات المرور التي يستخدمها لدخول حسابه أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 12: اختبار (كا2) للاستقلالية لتحديد الفروق في قوة كلمات المرور التي يستخدمها الطالب الجامعي حسب المستوى الدراسي

كلمات قوية	المستوى الدراسي	المجموع	قيمة اختبار	مستوى	القرار

وفريدة	ليسانس		ماستر			χ	الدلالة	
	F	%	F	%	F	%		
نعم	18	53	26	62	44	58	0.431	غير دال إحصائيا
لا	16	47	16	38	32	42		
المجموع	34	100	42	100	76	100		

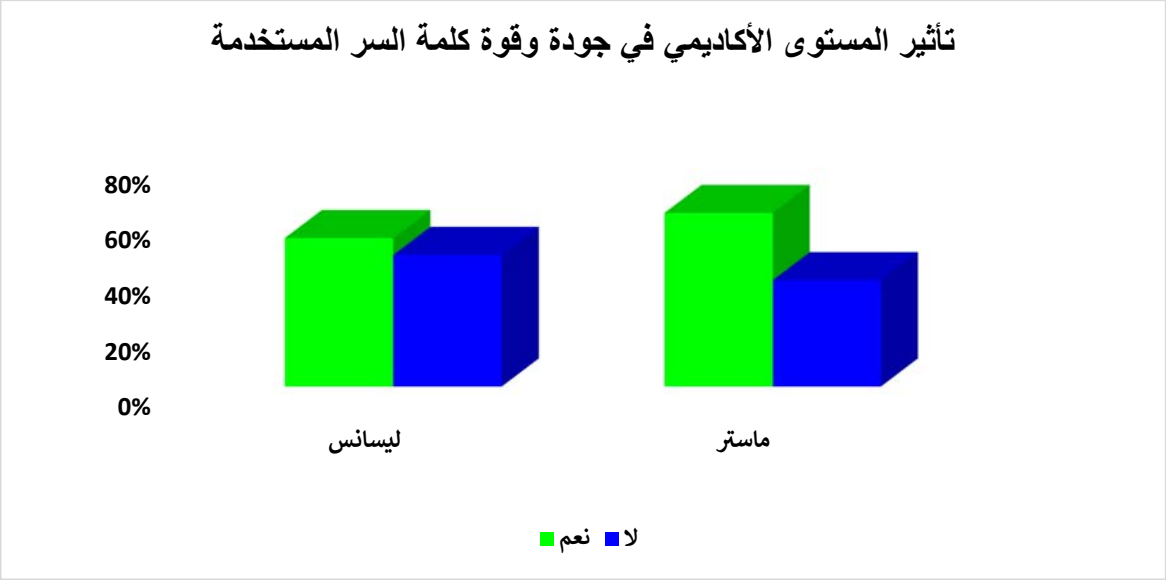
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة طلبة الليسانس: نجد أن 53% يلجأون إلى استخدام كلمات مرور قوية لحساباتهم، بينما 47% منهم لا يستخدمون كلمات قوية، بل مجرد كلمة مرور فقط.

أما بالنسبة لفئة طلبة الماستر: فنجد أن 62% يلجأون إلى استخدام كلمات مرور قوية لحساباتهم، في مقابل 38% منهم لا يستخدمون كلمات قوية، بل مجرد كلمة مرور فقط.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(0.61)** وهي قيمة غير دالة إحصائيا، وعلى هذا الأساس يمكن القول أن متغير المستوى الأكاديمي لا يؤثر على جودة وقوة كلمة السر المستخدمة لولوج حساب الطلبة الجامعيين،إذ نلحظ تقارب في تكرارات كلى المجموعتين.

والشكل الموالي يوضح الأمر أكثر.



الشكل 14: أعمدة بيانية للفروق في قوة كلمات المرور التي يستخدمها الطالب الجامعي حسب المستوى الدراسي

2. يؤثر متغير المستوى الدراسي في معرفة أساسيات الأمن السبراني.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كان المستوى الدراسي للطالب الجامعي يؤثر على معرفته لأساسيات الأمن السبراني أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 13: اختبار (كا2) للاستقلالية لتحديد الفروق في معرفة أساسيات الأمن السبراني لدى الطالب الجامعي حسب المستوى الدراسي

معرفة أساسيات الأمن السبراني	المستوى الدراسي				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	ليسانس		ماستر						
	F	%	F	%	F	%			
نعم	8	24	9	21	17	223	1.15	0.562	غير دال إحصائيا
لا	13	38	12	29	25	33			
إلى حد ما	13	38	21	50	34	45			
المجموع	34	100	42	55	76	100			

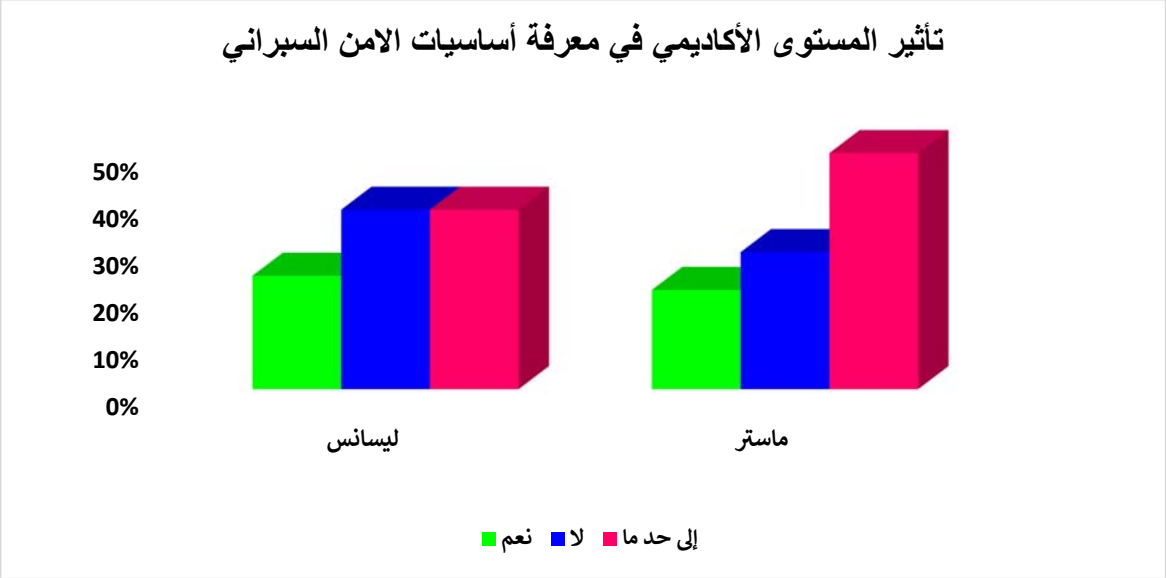
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة طلبة الليسانس: نجد أنه وبنسبة 38% تقاسمت فئتي الطلبة الذين (لا يعرفون أساسيات الأمن السبراني إطلاقا) مع (من يعرفون الأساسيات إلى حد ما)، بينما 24% منهم يجدون أنهم يعرفون حقا أساسيات الأمن السبراني.

أما بالنسبة لفئة طلبة الماستر: فنجد أن 50% منهم (من يعرفون أساسيات الأمن السبراني إلى حد ما)، بينما 29% منهم (لا يعرفون أساسيات الأمن السبراني إطلاقا)، في مقابل 21% منهم يجدون أنهم يعرفون حقا أساسيات الأمن السبراني.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(1.15)** وهي قيمة غير دالة إحصائيا، وعلى هذا الأساس يمكن القول أن متغير المستوى الأكاديمي لا يؤثر على مستوى معرفة ودراية الطالب الجامعي بأساسيات الأمن السبراني.

والشكل الموالي يوضح الأمر أكثر.



الشكل 15: أعمدة بيانية للفروق في معرفة أساسيات الأمن السبراني لدى الطالب الجامعي حسب المستوى الدراسي

3. يؤثر متغير الإقامة على تلقي تدريب أو محاضرات عن الأمن السبراني.

وللتحقق من صحة هذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كانت الإقامة تؤثر على تلقي الطالب لتدريب أو محاضرات عن الأمن السبراني أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 14: اختبار (كا2) للاستقلالية لتحديد الفروق في تلقي تدريب أو محاضرات عن الأمن السيبراني للطالب الجامعي حسب الإقامة

تلقي تدريب عن الأمن السبراني	الإقامة				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	مقيم		غير مقيم						
	F	%	F	%	F	%			
نعم	5	25	5	9	10	13	3.33	0.008	دال إحصائيا
لا	15	75	51	91	66	87			
المجموع	20	100	56	100	76	100			

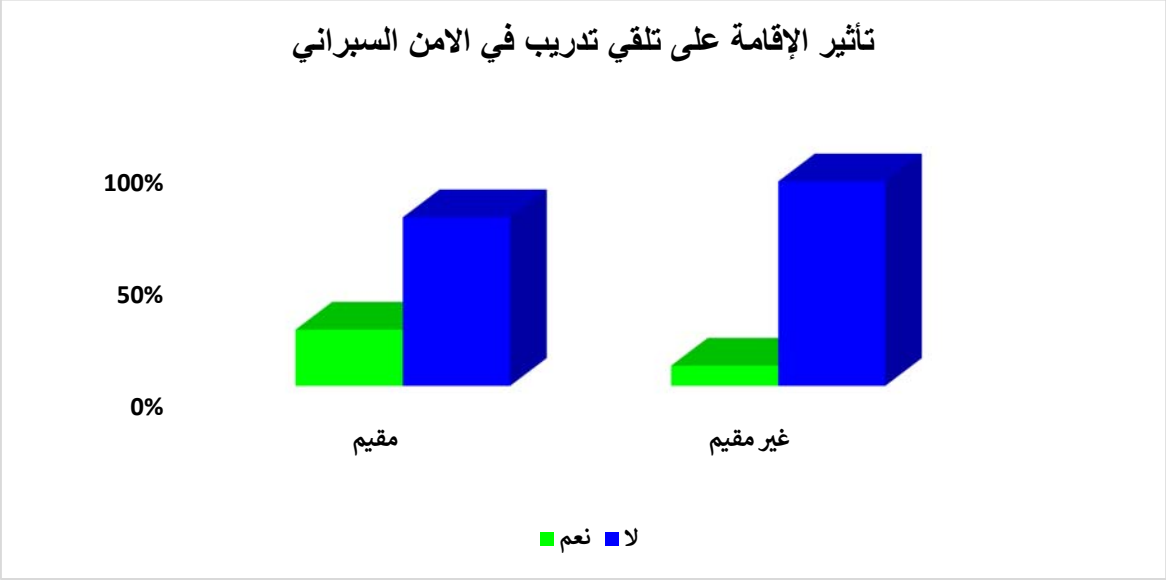
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الطلبة المقيمين: نجد أن 75% منهم يصرحون بأنهم لم يتلقوا أي تدريب حول الأمن السيبراني، في مقابل 25% منهم فقط من تلقوا هذا التدريب.

أما بالنسبة لفئة طلبة غير المقيمين: فنجد أن جلهم وبنسبة 91% منهم يصرحون بأنهم لم يتلقوا أي تدريب حول الأمن السيبراني، في مقابل 9% منهم فقط من تلقوا هذا التدريب.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(3.33)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α= 0.01)** ودرجة حرية **(df= 3)**، وعلى هذا الأساس يمكن القول أن متغير الإقامة يؤثر على تلقي الطالب الجامعي لتدريب حول الأمن السيبراني، حيث نجد أن الطلاب المقيمين هم أكثر الفئات التي تلقى أفرادها تدريب حول الأمن السيبراني.

والشكل الموالي يوضح الأمر أكثر.



الشكل 16: أعمدة بيانية للفروق في تلقي تدريب أو محاضرات عن الأمن السبراني للطالب الجامعي حسب الإقامة

4. يؤثر متغير الإقامة على تفعيل المصادقة الثنائية.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار **($كا^2$)** χ للاستقلالية، لتحديد ما إذا كان متغير الإقامة للطالب الجامعي يؤثر على تفعيله خاصية المصادقة الثنائية أم لا. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 15: اختبار (كا2) للاستقلالية لتحديد الفروق في تفعيل المصادقة الثنائية لدى الطالب الجامعي حسب الإقامة

تفعيل المصادقة الثنائية	الإقامة				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	مقيم		غير مقيم						
	F	%	F	%	F	%			
نعم	5	25	12	22	17	22	1.07	0.584	غير دال إحصائيا
لا	8	40	17	30	25	33			
إلى حد ما	7	35	27	48	34	45			
المجموع	20	100	56	100	76	100			

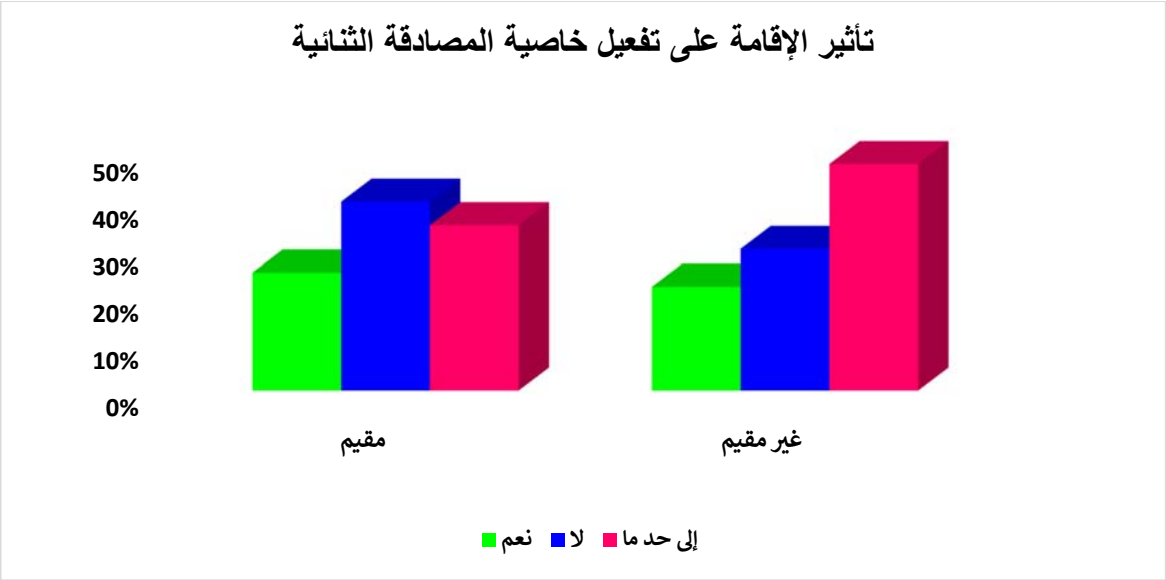
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الطلبة المقيمين: نجد أن 40% منهم يصرحون بأنهم لا يفعلو خاصية المصادقة الثنائية لحساباتهم، بينما 35% منهم يفعلون الخاصية إلى حد ما، في مقابل 25% منهم يصرحون أنهم يفعلون هذه الخاصية.

أما بالنسبة لفئة طلبة غير المقيمين: نجد أن 48% منهم يصرحون بأنهم خاصية المصادقة الثنائية لحساباتهم إلى حد ما بينما 30% منهم لا يفعلو خاصية المصادقة الثنائية لحساباتهم، فيما 22% منهم يصرحون أنهم يفعلون هذه الخاصية.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(1.07)** وهي قيمة غير دالة إحصائيا، اي انه لا توجد فروق دالة احصائيا في متغير تفعيل المصادقة الثنائية حسب متغير الاقامة

والشكل الموالي يوضح الأمر أكثر.



الشكل 17: أعمدة بيانية للفروق في تفعيل المصادقة الثنائية لدى الطالب الجامعي حسب الإقامة

3/ عرض نتائج محور الأمن السبراني والاحتيال الالكتروني:

1. العلاقة بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كانت هناك علاقة ارتباطية بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني لدى الطالب الجامعي. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 16: اختبار (كا2) للاستقلالية للعلاقة بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني

نوع الاحتيال	تلقى تدريب في الأمن السبراني				المجموع		قيمة اختبار χ	مستوى الدلالة	قيمة الارتباط
	نعم		لا						
	F	%	F	%	F	%			
مالي	0	0	7	11	7	9	9.79	0.002	0.75
عاطفي	1	9	7	11	8	11			
انتحال هوية	4	36	4	6	8	11			
غير ذلك	6	55	47	72	53	69			
المجموع	11	100	65	100	76	100			

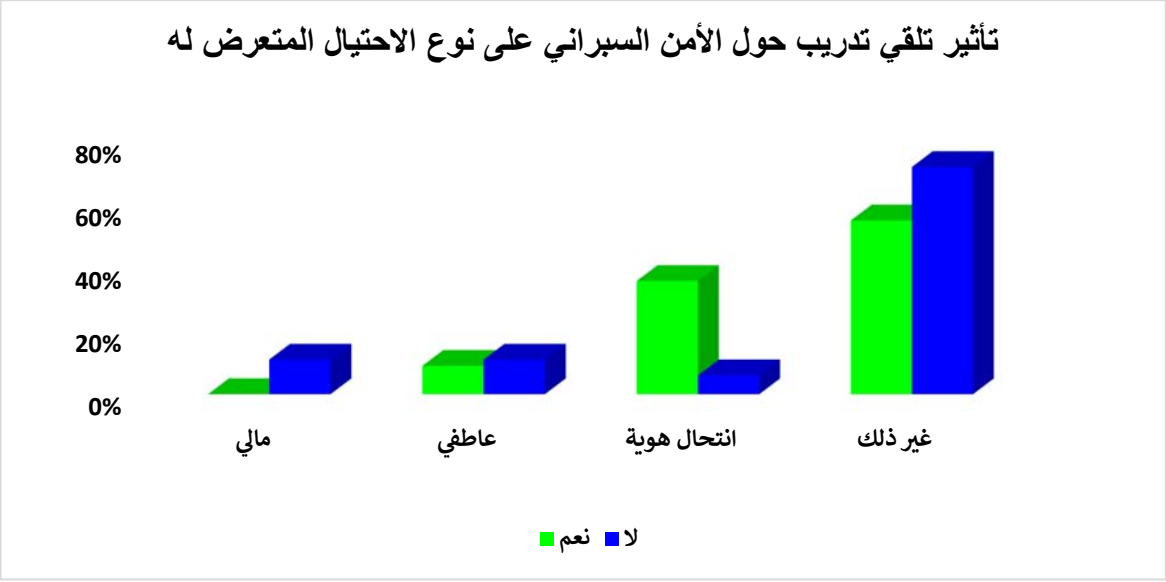
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الطلبة المتلقين لتدريب في الأمن السبراني: نجد أن 55% منهم يصرحون بأنهم تعرضوا لاحتيال من نوع آخر، بينما 36% منهم تعرضوا لانتحال هوية كنوع من الاحتيال، أما 9% منهم فتعرضوا لاحتيال عاطفي مع تسجيل غياب الاحتيال المالي لهذه الفئة.

أما بالنسبة لفئة الطلبة غير المتلقين لتدريب في الأمن السبراني: نجد أن 72% منهم يصرحون بأنهم تعرضوا لاحتيال من نوع آخر، بينما 11% منهم تعرضوا لاحتيال مالي ومثلها 11% متعرضين لاحتيال عاطفي، أما 9% منهم فتعرضوا لانتحال هوية كنوع من الاحتيال لهذه الفئة.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(9.79)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α= 0.01)**ودرجة حرية**(df= 3)**، وعلى هذا الأساس يمكن القول توجد فروق دالة احصائيا في متغير تلقي تدريب في الأمن السيبراني حسب نوع الاحتيال الذي تعرض له ، مع وجود علاقة دالة احصائيا قدرت ب 75 %بين تلقي تدريب في الأمن السبراني و نوع الاحتيال الذي تعرض الطالب الجامعي.

والشكل الموالي يوضح الأمر أكثر.



الشكل 18: أعمدة بيانية للعلاقة بين نوع الاحتيال الإلكتروني وتلقي تدريب في الأمن السبراني

2. العلاقة بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني.

وللتحقق من صحة هاذا الطرح تم اللجوء إلى اختبار (كا^2) χللاستقلالية، لتحديد ما إذا كانت هناك علاقة ارتباطية بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني لدى الطالب الجامعي. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 17: اختبار (كا2) للاستقلالية للعلاقة بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني

التصرف بعد التعرض للاحتيال	تلقى تدريب في الأمن السبراني				المجموع		قيمة اختبار χ	مستوى الدلالة	قيمة الارتباط
	نعم		لا						
	F	%	F	%	F	%			
التبليغ	3	30	2	3	5	7	19.48	0.000	0.81
حذف الحساب	3	30	7	11	10	13			
التجاهل	0	0	41	62	41	54			
غير ذلك	4	40	16	24	20	26			
المجموع	10	100	66	100	76	100			

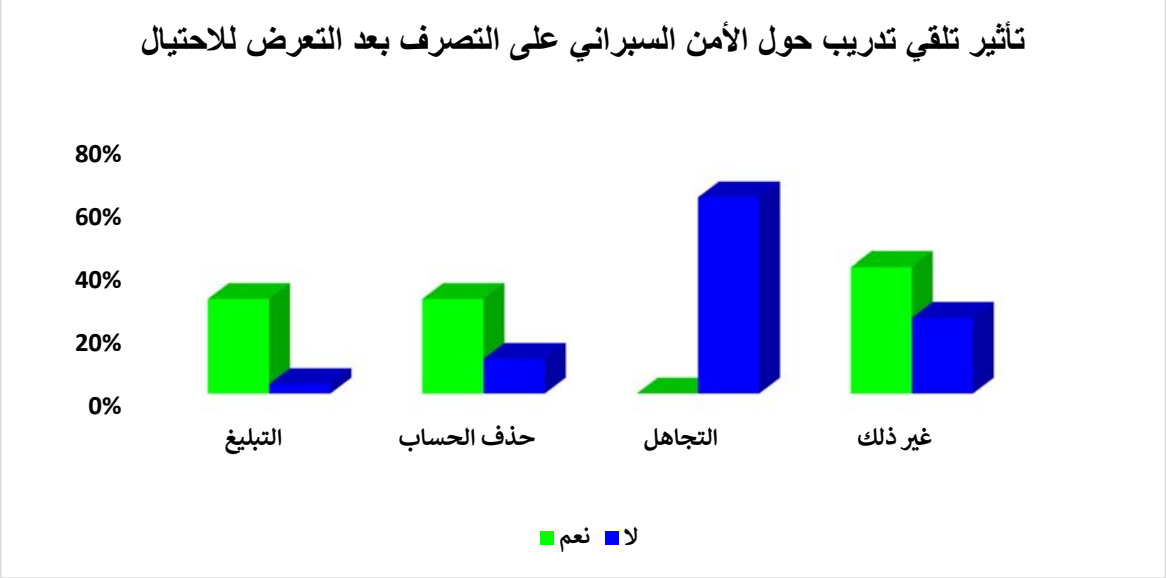
نلاحظ من خلال الجدول أعلاه أن:

بالنسبة لفئة الطلبة المتلقين لتدريب في الأمن السبراني: نجد أن 40% منهم يصرحون بأنهم تصرفوا بنوع آخر، بينما 30% منهم قاموا بالتبليغ، ومثلها 30% منهم قاموا بحذف الحساب، مع تسجيل غياب لتجاهل الموقف كتصرف بعد التعرض للاحتيال لدى هذه الفئة.

أما بالنسبة لفئة الطلبة غير المتلقين لتدريب في الأمن السبراني: نجد أن 62% منهم يصرحون بأنهم قاموا بتجاهل الموقف، بينما 24% منهم تصرفوا بنوع آخر، فيما 11% منهم قاموا بحذف الحساب، بينما 3% منهم فقط من قاموا بالتبليغ عن الاحتيال.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χالمحسوبة قدرت بـ **(19.48)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α =0.01)**ودرجة حرية**(df= 3)**، وعلى هذا الأساس يمكن القول أن متغير تلقي تدريب في الأمن السبراني يؤثر على التصرف مع موقف الاحتيال الذي تعرض الطالب الجامعي.

والشكل الموالي يوضح الأمر أكثر.



الشكل 19: أعمدة بيانية للعلاقة بين التصرف بعد التعرض للاحتيال وتلقي تدريب في الأمن السبراني

عرض نتائج الفرضية الأولى:

والتي مفادها: **هناك علاقة بين جهل الأفراد بمعرفة أساسيات الأمن السبراني، وزيادة تعرضهم لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي.**

وللتحقق من صحة هذا الطرح تم اللجوء إلى اختبار (كا^2) χ للاستقلالية، لتحديد ما إذا كان معرفة الطالب الجامعي لأساسيات الأمن السبراني يستقل عن تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي أم يرتبط به،. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 18: اختبار (كا2) للاستقلالية لتحديد العلاقة بين معرفة أساسيات الأمن السبراني لدى الطالب الجامعي وتعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي

معرفة أساسيات الأمن السبراني	التعرض للنصب والاحتيال				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	نعم		لا						
	F	%	F	%	F	%			
نعم	1	%2	16	%50	17	%22	19.63	0.000	الفرق دال إحصائيا
لا	22	%50	3	%9	25	%33			
إلى حد ما	21	%48	13	%41	34	%45			
المجموع	44	%100	32	%100	76	%100			

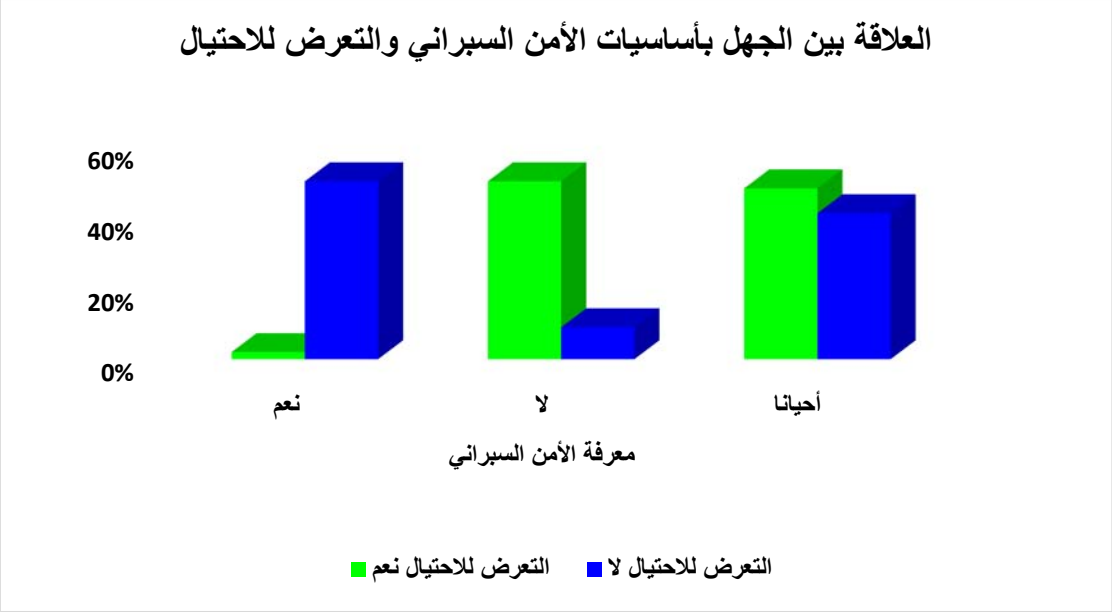
تظهر النتائج المدرجة في الجدول أعلاه أنه:

بالنسبة لفئة طلبة الذين يعرفون أساسيات الأمن السبراني: بالرجوع لوضعية التعرض للنصب والاحتيال على مواقع التواصل الاجتماعي نجد أن 16 فرد لم يتعرضوا لأي نصب أو احتيال عبر المواقع بما نسبته: 50% من مجموع من لم يتعرضوا للنصب والاحتيال، فيما تعرض فقط 3% منهم إلى أحد أنواع النصب والاحتيال عبر أحد مواقع التواصل الاجتماعي من مجموع الطلبة المتعرضين للاحتيال.

بالنسبة لفئة طلبة الذين يجهلون أساسيات الأمن السبراني: بالرجوع لوضعية التعرض للنصب والاحتيال على مواقع التواصل الاجتماعي نجد أن 22 فرد يصرحون أنهم يتعرضوا لأحد أنواع النصب والاحتيال عبر أحد مواقع التواصل الاجتماعي، أي بنسبة 50% من مجموع الطلبة المتعرضين للاحتيال، فيما نجد فقط 3% منهم لم يتعرضوا للنصب والاحتيال، من مجموع من لم يتعرضوا للنصب والاحتيال عبر أحد مواقع التواصل الاجتماعي.

بالنسبة لفئة طلبة الذين يعرفون أساسيات الأمن السبراني إلى حد ما: بالرجوع لوضعية التعرض للنصب والاحتيال على مواقع التواصل الاجتماعي نجد أن 21 فرد تعرضوا للنصب واحتيال عبر المواقع بما نسبته: 48% من مجموع الطلبة المتعرضين للنصب والاحتيال، بينما 41% منهم لم يتعرضوا إلى أي أنواع النصب والاحتيال عبر أحد مواقع التواصل الاجتماعي من مجموع الطلبة غير المتعرضين للاحتيال.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(19.63)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α= 0.01)** ودرجة حرية **(df= 2)**، وعلى هذا الأساس يمكن القول أنه: **توجد علاقة بين جهل الأفراد بمعرفة أساسيات الأمن السبراني، وزيادة تعرضهم لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي**، حيث كلما زادت معرفة الطالب بأساسيات الأمن السبراني انخفض تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي، والعكس صحيح، فكلما زاد جهل الطالب بأساسيات الأمن السبراني ارتفع تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي، **وعليه نقبل الفرضية الأولى. والشكل الموالي يوضح ذلك:**



الشكل20: أعمدة بيانية لتوضيح العلاقة بين معرفية أساسيات الأمن السبراني لدى الطالب الجامعي وتعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي

عرض نتائج الفرضية الثانية:

والتي مفادها: **تؤثر عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي.**

وللتحقق من صحة هذا الطرح تم اللجوء إلى اختبار (χ^2 **كا**) للاستقلالية، لتحديد ما إذا كان تحكم الطالب الجامعي في التكنولوجيا يستقل عن تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي أم يرتبط به،. وتمثلت النتائج كما هي موضحة في الجدول الموالي:

الجدول 19: اختبار (كا2) للاستقلالية لتحديد تأثير عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي.

عدم التحكم في التكنولوجيا	التعرض للنصب والاحتيال				المجموع		قيمة اختبار χ	مستوى الدلالة	القرار
	نعم		لا						
	F	%	F	%	F	%			
نعم	31	%70	13	%42	44	%58	23.27	0.000	الفرق دال إحصائيا
لا	13	%30	19	%58	32	%42			
المجموع	44	%100	32	%100	76	%100			

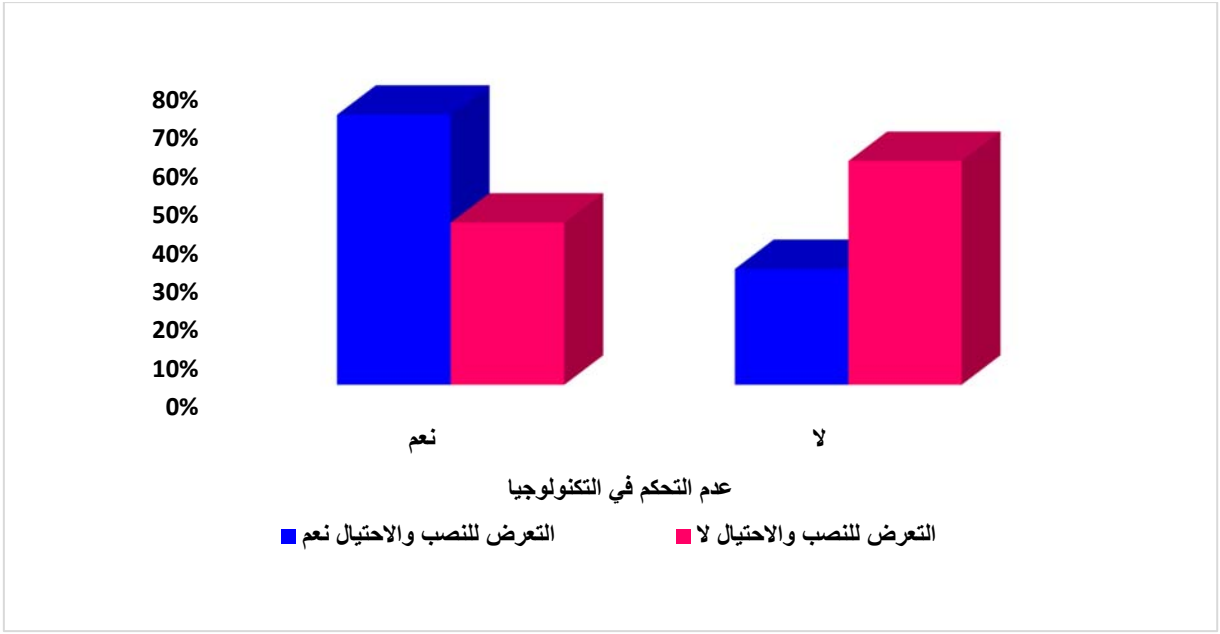
تظهر النتائج المدرجة في الجدول أعلاه أنه:

بالنسبة لفئة طلبة الذين المتعرضين للنصب والاحتيال الالكتروني: تظهر النتائج أن 70% من أفراد هذه الفئة نجدهم غير متحكمين في التكنولوجيا، بينما 30% من أفراد هذه الفئة هم من لهم القدرة على التحكم في التكنولوجيا.

بالنسبة لفئة طلبة غير المتعرضين للنصب والاحتيال الالكتروني: تظهر النتائج أن 58% من أفراد هذه الفئة نجدهم لهم القدرة على التحكم في التكنولوجيا، بينما 44% من أفراد هذه الفئة هم من غير متحكمين في التكنولوجيا.

وبالعودة للعامل الإحصائي نجد أن قيمة اختبار χ المحسوبة قدرت بـ **(23.27)** وهي قيمة دالة إحصائيا عند مستوى الدلالة **(α= 0.01)** ودرجة حرية **(df= 1)**، وعلى هذا الأساس يمكن القول أنه: **تؤثر عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي،** حيث كلما زاد جهل الطالب بالتحكم في التكنولوجيات الحديثة زاد معها تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي، والعكس صحيح، فكلما زاد تحكم الطالب في التكنولوجيات الحديثة قل معها تعرضه للنصب والاحتيال عبر مواقع التواصل الاجتماعي، **وعليه نقبل الفرضية الثانية.**

والشكل الموالي يوضح ذلك:



الشكل 21: أعمدة بيانية لتوضيح تأثير عدم القدرة على التحكم في التكنولوجيا على زيادة تعرض الأفراد لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي.

نتائج الفرضيات:

- **نتائج الفرضية الأولى:**

نستنتج أن توجد علاقة بين جهل الأفراد بالأمن السيبراني وزيادة تعرضهم لجرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي .

أثبتت الدراسة الميدانية صحة هذه الفرضية ، حيث أظهرت البيانات أن غالبية الأفراد الذين لم يتلقوا تكوينا أو توجيها في مجال الأمن السيبراني كانوا أكثر عرضة للاحتيال الالكتروني.وقد تنوعت أشكال الاحتيال التي تعرضوا لها ، مثل انتحال الهوية ،الرسائل المزيفة ، والعروض الوهمية .

العلاقة طردية موجبة ، فكلما انخفض الوعي بالأمن السيبراني ارتفعت احتمالات الوقوع ضحية لاحتيال .

أظهرت نتائج الدراسة أن نسبة معتبرة من الطلبة الذين لم يسبق لهم تكوين أو توعية حول الأمن السيبراني كانوا أكثر عرضة لجرائم النصب والاحتيال عبر الانترنت وأبرز أشكال الاحتيال التي تعرضوا لها تمثلت في:

- انتحال الهوية من قبل المحتالين.
- الروابط المزيفة.
- الرسائل الاحتيالية المرتبطة بمسابقات وهمية
- عروض عمل كاذبة.

- **نتائج الفرضية الثانية:**

نستنتج أن :

تؤثر عدم القدرة على التحكم التكنولوجي على زيادة تعرض الأفراد للاحتيال عبر مواقع التواصل الاجتماعي .

أكدت المعطيات الميدانية أن الطلبة الذين يواجهون صعوبات في استخدام الأدوات التقنية أو لا يتحكمون في إعدادات الأمان والخصوصية ، كانوا أكثر عرضة للوقوع في فخاخ النصب الرقمي .كما لوحظ أن هذه الفئة تميل إلى التفاعل الساذج معا محتويات مضللة أوروابط مجهولة المصدر .

العلاقة عكسية ، أي كلما ضعفت القدرة على استخدام التكنولوجيا بوعي زادت احتمالات الاستهداف والوقوع ضحية للاحتيال .

بينت الدراسة أن الطلبة الذين أظهروا ضعفا في استخدام تقنيات المنصات الاجتماعية أو التعامل مع إعدادات الخصوصية والأمان ، كانوا أكثر عرضة للاستهداف من قبل المحتالين ومن بين أهم المؤشرات:

- النقر العشوائي
- القبول السريع لطلبات الصداقة من مجهولين.
- التفاعل السريع لطلبات الصداقة من مجهولين.
- مشاركة بيانات مهمة دون التحقق من الهوية الرقمية للطرف الأخر.

الاستنتاج العام:

من خلال الدراسة النظرية والميدانية ، تبين ان جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي تمثل تهديدا حقيقيا لفئة الطلبة الجامعيين ، خاصة في ظل الاستخدام المكثف وغير الوعي للفضاء الرقمي . وقد أثبتت نتائج البحث أن هناك علاقة واضحة بين ضعف الوعي بالأمن السيبراني وقلة المهارات التقنية من جهة ، وبين قابلية الأفراد للتعرض للاحتيال الالكتروني من جهة أخرى .

كما أوضحت الدراسة أن الهندسة الاجتماعية تعد من أبرز الأساليب التي يعتمدها المحتالين للايقاع بالضحايا ، عبر استغلال الثقة ، والاندفاع، وسوء تقدير المخاطر.

وأظهرت البيانات أن غياب التكوين والتوعية الرقمية يضاعف من فرص الوقوع ضحية .

وبناء عليه ، فإن مواجهة هذه الظاهرة تتطلب تضافر الجهود التربوية والتثقيفية ، وتعزيز ثقافة الحماية الرقمية داخل المؤسسات الجامعية، إلى جانب تطوير آليات قانونية وتشريعية تحمي المستخدمين في البيئة الافتراضية .

خاتمة

خاتمة:

في ضوء ما توصلت إليه هذه الدراسة، يتبين أن ظاهرة النصب والاحتيال عبر مواقع التواصل الاجتماعي لم تعد مجرد حالات فردية، بل أصبحت شكلا متطورا من الانحراف الاجتماعي في العصر الرقمي، يستدعي الدراسة والتحليل من زوايا متعددة. وقد أثبتت نتائج البحث الميداني وجود علاقة وثيقة بين كل من الجهل بالأمن السيبراني، وضعف التحكم في استخدام التكنولوجيا، وزيادة احتمالات الوقوع ضحية للاحتيال الالكتروني، خاصة في أوساط الشباب الجامعي.

لقد ساهمت هذه الدراسة في تقديم قراءة سوسيولوجية لواقع الضحايا، مبرزة كيف تؤثر العوامل النفسية والاجتماعية والرقمية على قابلية الفرد للاستهداف، مستندة في ذلك إلى نظريتي الأنشطة الروتينية وأسلوب الحياة. كما أكدت على أهمية الوقاية الرقمية وضرورة إدماج مفاهيم الأمن السيبراني ضمن التكوين الجامعي.

وختاما فإن مواجهة هذه الظاهرة تتطلب تظافر جهود الأسرة، والمؤسسات التربوية والسلطات التشريعية، من أجل بناء ثقافة رقمية واعية تحمي الأفراد من الوقوع ضحايا في الفضاء الافتراضي.

قائمة المصادر و المراجع

قائمة المراجع والمصادر:

1/*القرآن الكريم:

سورة الأنبياء، الآية 18.

سورة مريم ، الآية 46.

2/* الكتب:

[1]– أحمد مصطفى محمد: مناهج البحث العلمي بين النظرية والتطبيق، القاهرة، مصر ط 2، دار الوفاء لدنيا الطباعة والنشر، 2008.

[2]–خضر حسن الحسين سيد : أساسيات البحث العلمي في العلوم الاجتماعية والإنسانية، القاهرة، مصر ط 1 ، دار المعرفة الجامعية ، 2014.

[3]– محمد عبد السلام و، عادل محمد الشر بجي: الجريمة **الالكترونية في الفضاء الالكتروني المفهوم– الأسباب**– سبل مكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات السداسية، العدد 04، سنة 2019.

[4]– رشيد زرواتي : **تدريبات على منهجية البحث العلمي في العلوم الاجتماعية** ، الجزائر ، ديوان المطبوعات الجامعية 2008.

[5]– سوا كري الطاهر ، **نمطية الجريمة في المجتمع الجزائري** ، مخبر الجريمة والانحراف بين الثقافة و التماثلات الاجتماعية .ط1. 2022.

[6]– سامر سلمان الجبوري ، **جريمة الاحتيال الالكتروني** ، منشورات زين، الحقوقية ، بيروت لبنان ، الطبعة الأولى 2018.

[7]– طارق عفيفي، صادق أحمد، **الجرائم الالكترونية (جرائم الهاتف المحمول)**، الطبعة الأولى 2015.

[8]– طارق عفيفي صادق أحمد ، الجرائم الالكترونية جرائم الهاتف المحمول ، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي ،محاضر منتدى بجامعة حلوان عضو الجمعية المصرية للاقتصاد السياسي والتشريع عضو الجمعية –المصرية للقانون الدولي–القاهرة– الطبعة الأولى 2015.

[9]–عقل حسن حسين: **مناهج البحث العلمي**، الأسس والتطبيقات، بيروت لبنان ، ط1 ، دار الفكر العربي 2006.

10–عبد العال الديبري، **الجرائم الالكترونية** ، المركز القومي للإصدارات القانونية .الطبعة الأولى 2012.

11-دينا عبد العزيز فهمي – "**المسؤولية الجنائية الناشئة عن استخدام مواقع التواصل الاجتماعي**" : مجلة الحقوق للبحوث القانونية والاقتصادية ،م3، المجلد 2019 ،2،العدد2 يوليو 2019 .

12-محمد سرحان علي المحمودي: **مناهج البحث العلمي** ، الجمهورية اليمنية صنعاء ، ط 3 ، دار الكتب 2019.

13- ملحم سامي محمد : مناهج **البحث العلمي في العلوم التربوية والنفسية** ، عمان الأردن ، ط 3 دار النشر المسيرة للنشر والتوزيع.

14-محمد الصاوي محمد مبارك : **البحث العلمي أسسه وطريقة كتابته** ، القاهرة ،مؤسسة الإسراء للنشر والتوزيع ط1.

15-محمد عبد العال النعيمي وآخرون: **طرق ومناهج البحث العلمي** ،عمان، الوراق للنشر والتوزيع ،2015.

16-يوسف عبد الأمير طباجة : **منهجية البحث تقنيات ومناهج** ، بيروت ، دار الهادي للطباعة والنشر والتوزيع 2007.

3/مذكرات ورسائل:

1- الطالبة نايري عائشة ،**الجريمة الالكترونية في التشريع الجزائري** ، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية ، جامعة أحمد درية – أدرار. 2016-2017.

2- بوكساني شيراز وسرحان شيماء : **جريمة النصب والاحتيال عبر مواقع التوصل الاجتماعي** ، مذكرة لنيل شهادة ماستر في القانون ، كلية الحقوق بودواو ، جامعة احمد بوقره – بومرداس ، 2023/2022م.

3- جريمة الابتزاز الالكتروني، دراسة ميدانية علمية.طلبة جامعة المدية . العلوم القانونية والاجتماعية.

4- حاجي سميرة و مريش رقية: جريمة النصب والاحتيال في التشريع الجزائري ، مذكرة لنيل شهادة الماستر جامعة محمد بوضياف – المسيلة ، 2023/2022.

5- عباس زكرياء : **ضحايا جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي** ،مذكرة مقدمة لنيل شهادة الماستر في علم الاجتماع جريمة وانحراف ،كلية العلوم الإنسانية والاجتماعية ، جامعة جيلا لي بونعامة خميس مليانة، 2023/2022.

6- لموشي جهيدة ، طالبة دكتوراه، **دور الضحية في حدوث الجريمة النصب والاحتيال** –مقاربة سوسيولوجية ، كلية الآداب والعلوم الإنسانية والاجتماعية ، جامعة باجي مختار عنابة .ص 252-253.

7- مهدي ربوح ، زكرياء العيشي ، **العوامل المؤدية لوقوع جرائم النصب والاحتيال عبر مواقع التواصل الاجتماعي الفايسبوك نموذجا**،مذكرة مكملة لنيل ما ستر في تخصص علم الاجتماع الانحراف والجريمة كلية العلوم الاجتماعية والإنسانية ، جامعة الكلي محمد او لحاح بالبويرة ، سنة 2021-2022.

4/المجلات:

1- الشيخ عبد العزيز بن عبد الرحمان بن سعد البشرمي : **جريمة النصب والاحتيال** ، مكة المكرمة، مجلة العدد 391 ، رجب 1429 هجري.

2- جمال نسيب،لامية بوبيدي، **قراءة سوسيو نقدية لمضامين بعض النظريات السوسولوجية الحديثة المفسرة للجريمة:الاختيار العقلاني،أسلوب الحياة والنشاط الرتيبي نموذجا** ، مجلة الدراسات وأبحاث المجلة العربية في العلوم الإنسانية والاجتماعية2022.

3- دينا عبد العزيز فهمي – "**المسؤولية الجنائية الناشئة عن استخدام مواقع التواصل الاجتماعي**" : مجلة الحقوق للبحوث القانونية والاقتصادية ،م3، المجلد 2019 ،2،العدد2 يوليو 2019.

4- شفيقة خنيفر،المؤتمر العلمي الافتراضي الأول: **الجريمة الالكترونية (الواقع والتحديات) عنوان المداخلة الاجرام الالكتروني، كفاءات ضائعة في عالم التقنية** ، جامعة محمد الشريف مساعديه ، سوق أهراس.

5- عفاف بعون، نسيمة أولاد سالم، **الجريمة الالكترونية –قراءة سوسيو تاريخية في النشأة والآثار**، مجلة القبس للدراسات النفسية والاجتماعية /المجلد (05) العدد (20) 2023 .

6- صبرينة رماش ، **تحليل سلوك ضحايا جريمة النصب والاحتيال والعوامل المحيطة بهم وفق نظرية الأنشطة الروتينية** ، مجلة الرسالة للدراسات والسلوك والبحوث الإنسانية ، جامعة باجي مختارعنابة الجزائر ،2024وزي : علم الضحايا و إسهاماته في الحقل الجنائي ، مجلة الفنون.

7- يمينة لعبيدي: **تحليل سلوك ضحايا جريمة النصب والاحتيال والعوامل المحيطة بها**، مجلة الدراسات.

5/ المواقع الالكترونية:

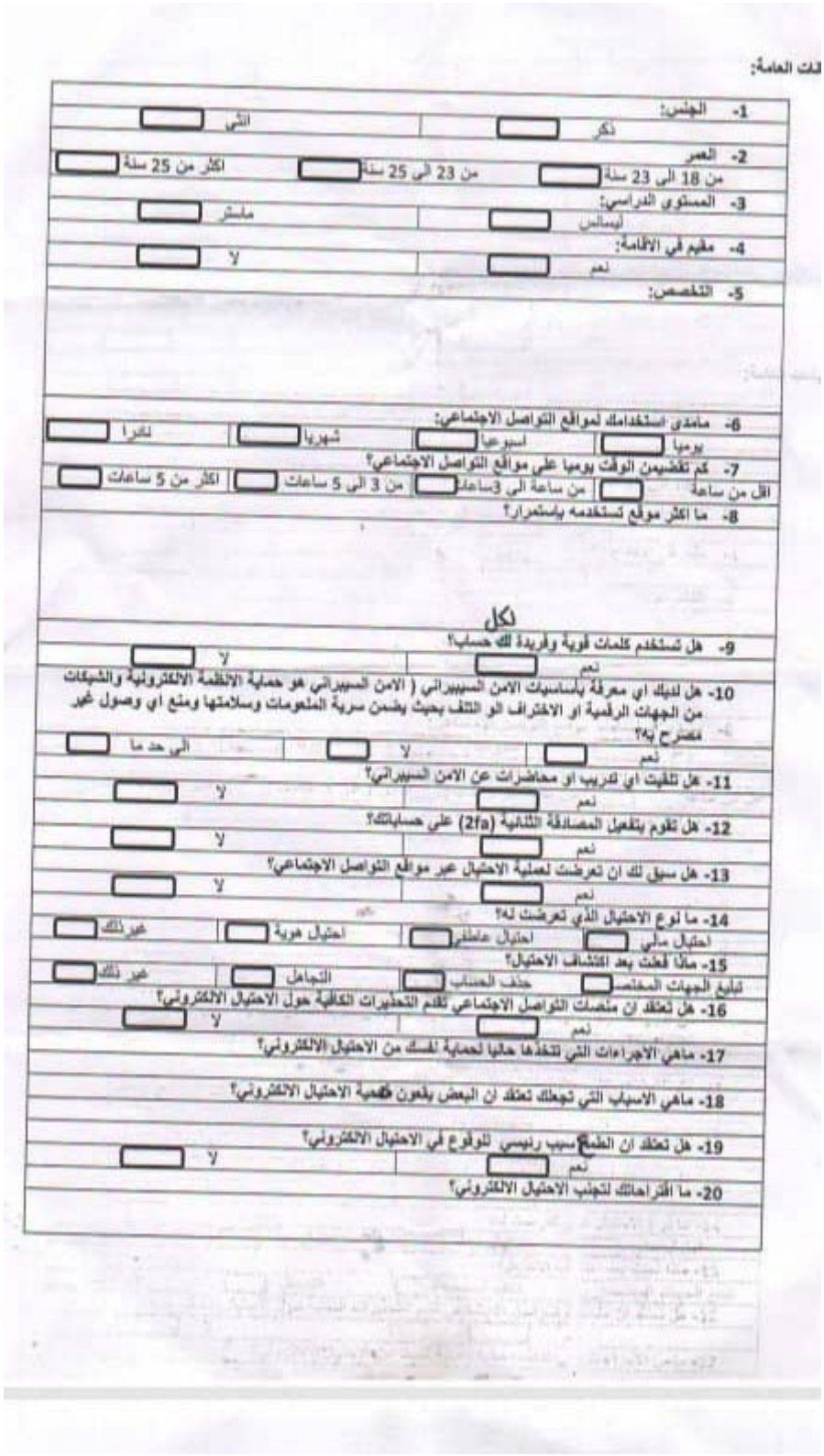
1- http:/: ar. Wikipedia .org

2-http://www.maktabtk.com

3- محمد هادي ،**الجرائم الالكترونية ،تهدد مستقبل أباتنا** 2024 WWW.aljazeera-net.02/09 شوهد في 4 مارس 2025- على الساعة 10.52.

4- جريمة النصب والاحتيال في القانون الجزائري، محاضرة، شوهد يوم 2025/05/20، على الساعة 10.00 moodle.université-eltarf.dz

قائمة الملاحق



لات العامة:

1- الجنس:
ذكر ☐ انثى ☐

2- العمر
من 18 الى 23 سنة ☐ من 23 الى 25 سنة ☐ اكثر من 25 سنة ☐

3- المستوى الدراسي:
ليسانس ☐ ماستر ☐

4- مقيم في الاقامة:
نعم ☐ لا ☐

5- التخصص:

6- مامدى استخدامك لمواقع التواصل الاجتماعي:
يوميا ☐ اسبوعيا ☐ شهريا ☐ نادرا ☐

7- كم تقضيمن الوقت يوميا على مواقع التواصل الاجتماعي؟
اقل من ساعة ☐ من ساعة الى 3ساعات ☐ من 3 الى 5 ساعات ☐ اكثر من 5 ساعات ☐

8- ما اكثر موقع تستخدمه باستمرار؟

لكل

9- هل تستخدم كلمات قوية وفريدة لك حساب؟
نعم ☐ لا ☐

10- هل لديك اي معرفة بأساسيات الامن السيبيراني (الامن السيبيراني هو حماية الانظمة الالكترونية والشبكات من الجهات الرقمية او الاختراف او التلف بحيث يضمن سرية المعلومات وسلامتها ومنع اي وصول غير مصرح به؟
نعم ☐ لا ☐ الى حد ما ☐

11- هل تلقيت اي تدريب او محاضرات عن الامن السيبيراني؟
نعم ☐ لا ☐

12- هل تقوم بتفعيل المصادقة الثنائية (2fa) على حساباتك؟
نعم ☐ لا ☐

13- هل سبق لك ان تعرضت لعملية الاحتيال عبر مواقع التواصل الاجتماعي؟
نعم ☐ لا ☐

14- ما نوع الاحتيال الذي تعرضت له؟
احتيال مالي ☐ احتيال عاطفي ☐ احتيال هوية ☐ غير ذلك ☐

15- ماذا فعلت بعد اكتشاف الاحتيال؟
تبليغ الجهات المختصة ☐ حذف الحساب ☐ التجاهل ☐ غير ذلك ☐

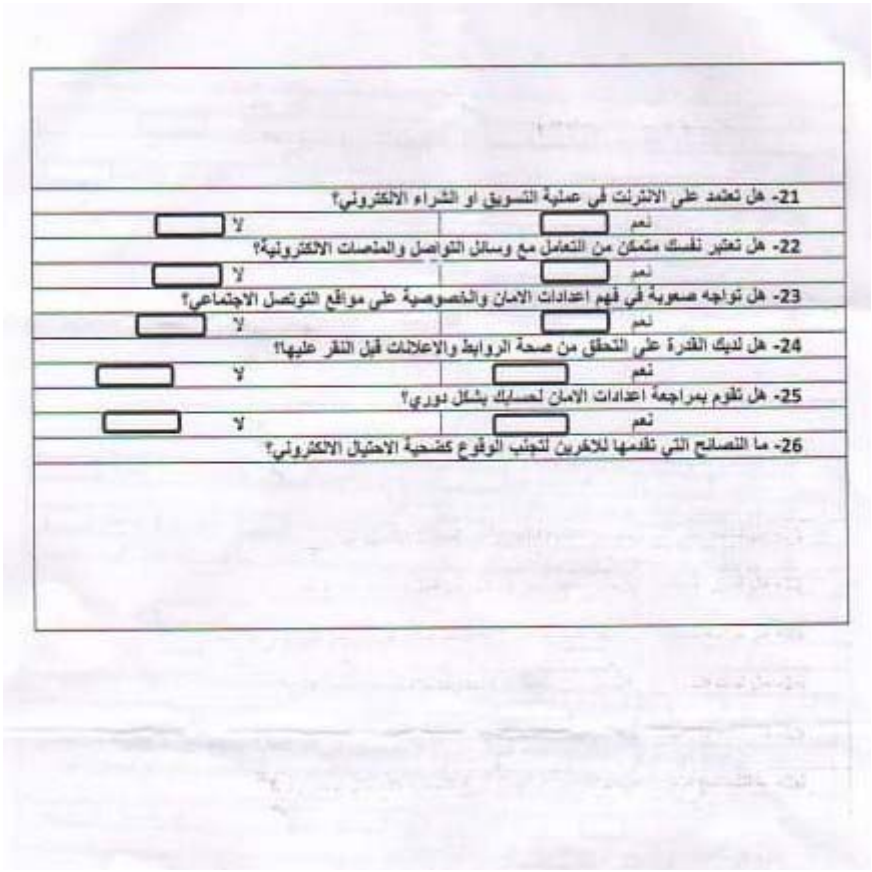
16- هل تعتقد ان منصات التواصل الاجتماعي تقدم التحذيرات الكافية حول الاحتيال الالكتروني؟
نعم ☐ لا ☐

17- ماهي الاجراءات التي تتخذها حاليا لحماية نفسك من الاحتيال الالكتروني؟

18- ماهي الاسباب التي تجعلك تعتقد ان البعض يقعون ضحية الاحتيال الالكتروني؟

19- هل تعتقد ان الطمع سبب رئيسي للوقوع في الاحتيال الالكتروني؟
نعم ☐ لا ☐

20- ما اقتراحاتك لتجنب الاحتيال الالكتروني؟



21- هل تعتمد على الانترنت في عملية التسوق او الشراء الالكتروني؟

نعم ☐ لا ☐

22- هل تعتبر نفسك متمكن من التعامل مع وسائل التواصل والمنصات الالكترونية؟

نعم ☐ لا ☐

23- هل تواجه صعوبة في فهم اعدادات الامان والخصوصية على مواقع التواصل الاجتماعي؟

نعم ☐ لا ☐

24- هل لديك القدرة على التحقق من صحة الروابط والاعلانات قبل النقر عليها؟

نعم ☐ لا ☐

25- هل تقوم بمراجعة اعدادات الامان لحسابك بشكل دوري؟

نعم ☐ لا ☐

26- ما النصائح التي تقدمها للاخرين لتجنب الوقوع كضحية الاحتيال الالكتروني؟