بسم الله الرحمن الرحيم
Omdurman Islamic University Journal of Applied Sciences
(OIUJ)-(ASC)
للعلوم التطبيقية مجلة جامعة أم درمان الاسلامية
https://journal.oiu.edu.sd/index.php/oiuj
https://doi.org/ 10.52981/oiujas.v22i2.3662
ISSN: 3122-5640
2026; 22(2)149-185

# النصب الإلكتروني عبر المنصات الرقمية: دراسة تحليلية لأسبابه، آثاره واستراتيجيات الوقاية

**محمود محمد احمد حامد علي1**

[1]مركز معلومات ولاية نهرالنيل (مكتب الوالي) ، أمانة الحكومة – الدامر، ولاية نهر النيل، جمهورية السودان

**البريد الالكتروني : alnfeedabi@gmail.com**

**للاستشهاد بهذا المقال:-**

**محمود محمد احمد حامد علي، النصب الإلكتروني عبر المنصات الرقمية: دراسة تحليلية لأسبابه، آثاره واستراتيجيات الوقاية، مجلة جامعة أم درمان الاسلامية للعلوم التطبيقية**

**ISSN: 3122-5640**

https://doi.org/10.52981/oiuj.v22i2.3662

**المستخلص:**

هدفت هذه الدراسة إلى تحليل طبيعة العلاقة بين الوعي الرقمي لدى المستخدمين، العوامل النفسية والاجتماعية، وأساليب النصب الإلكتروني، وتقييم فعالية استراتيجيات الوقاية والحماية الرقمية في السودان. وقد اعتمدت الدراسة المنهج الوصفي التحليلي، واستخدمت استبانة لجمع البيانات من عينة مكونة من 217 مستخدمًا للمنصات الرقمية. أظهرت النتائج وجود علاقة عكسية ذات دلالة إحصائية بين مستوى الوعي الرقمي واحتمالية التعرض للنصب الإلكتروني، في حين أظهرت العوامل النفسية والاجتماعية تأثيرًا إيجابيًا في زيادة التعرض للانتهاكات الرقمية. كما أظهرت النتائج أن أساليب النصب الإلكتروني الحديثة مرتبطة بخسائر مالية ونفسية واجتماعية ملموسة، وأن استراتيجيات الوقاية الرقمية تسهم بفاعلية في الحد من هذه المخاطر. وأكدت الدراسة على أهمية تعزيز الإطار التشريعي لحماية البيانات الشخصية، تحديث قوانين جرائم المعلوماتية، وإقرار قانون للأمن الجنائي الرقمي، إلى جانب توسيع برامج التوعية الرقمية والتعليمية لتعزيز الثقافة الرقمية وحماية المستخدمين.

**الكلمات المفتاحية:**الوعي الرقمي، النصب الإلكتروني، العوامل النفسية والاجتماعية، الأمن السيبراني، الحماية الرقمية، السودان.

**Abstract:**

This study aimed to analyze the relationship between users' digital awareness, psychological and social factors, and electronic fraud schemes, while evaluating the effectiveness of digital prevention and protection strategies in Sudan. The study employed a descriptive-analytical methodology and collected data through a structured questionnaire administered to a sample of 217 digital platform users. The results revealed a statistically significant inverse relationship between digital awareness and susceptibility to electronic fraud, whereas psychological and social factors positively influenced exposure to digital violations. Furthermore, modern electronic fraud schemes were associated with tangible financial, psychological, and social losses. The findings also indicated that preventive digital strategies effectively mitigate these risks. The study emphasizes the importance of strengthening the legislative framework for personal data protection, updating the Sudanese Cybercrime Law, enacting digital criminal security regulations, and expanding digital awareness and educational programs to enhance digital literacy and protect users.

**Keywords:** Digital Awareness, Electronic Fraud, Psychological and Social Factors, Cybersecurity, Digital Protection, Sudan.

# 1. الإطار المنهجي والدراسات السابقة

## اولاً: الإطار المنهجي:

### المقدمة:

شهدت السنوات الأخيرة انتشارًا واسعًا للمنصات الرقمية، مثل فيسبوك وواتساب وإنستغرام، لتصبح جزءًا أساسيًا من الحياة اليومية للأفراد والمجتمعات. فقد باتت هذه المنصات وسيلة رئيسية للتواصل الاجتماعي، والتسويق الإلكتروني، والتجارة، ونقل المعلومات. ومع هذا الانتشار الكبير، ظهرت تحديات جديدة تهدد المستخدمين، من أبرزها النصب الإلكتروني، الذي أصبح ظاهرة خطيرة في الفضاء الرقمي المعاصر.

يعرف النصب الإلكتروني على أنه كل عملية احتيال يتم تنفيذها عبر الإنترنت بهدف الحصول على أموال، أو بيانات شخصية، أو معلومات حساسة بطريقة مضللة أو خادعة. ويعتمد المحتالون في غالب الأحيان على الهندسة الاجتماعية لاستغلال الثغرات السلوكية والنفسية للمستخدمين، مثل الضغط على الروابط المزيفة، أو مشاركة رمز التحقق، أو الانخداع بالعروض الوهمية والفوز بالجوائز.

تكمن خطورة النصب الإلكتروني في أنه لا يؤدي فقط إلى خسائر مالية، بل يمتد أثره ليشمل الانتهاك المحتمل للخصوصية، والتأثير على الثقة بين الأفراد، وزيادة حالات الابتزاز الرقمي، إلى جانب الآثار النفسية والاجتماعية التي قد تنعكس على جودة حياة المستخدمين. وعليه، فإن ظاهرة النصب الإلكتروني تمثل تحديًا كبيرًا للحكومات، والمنصات الرقمية، والمجتمع بشكل عام، وتستدعي الدراسة والتحليل لفهم أسبابها وطرق مواجهتها.

وعلى الرغم من الجهود المبذولة للحد من هذه الظاهرة، سواء من خلال تطوير أدوات الحماية على المنصات أو سن قوانين وتشريعات وطنية لمكافحة الجرائم الإلكترونية، فإن العديد من المستخدمين لا يزالون عرضة للنصب بسبب ضعف الوعي الرقمي، أو قلة المعرفة بأساسيات الأمن السيبراني، أو غياب الثقافة الوقائية الرقمية.

تسعى هذه الدراسة إلى تقديم تحليل شامل للنصب الإلكتروني على المنصات الرقمية، من خلال تحديد أشكال وأساليب الاحتيال، دراسة العوامل النفسية والاجتماعية التي تزيد من تعرض المستخدمين، تقييم الأثر الاقتصادي والاجتماعي لهذه الظاهرة، واستعراض أفضل الممارسات والاستراتيجيات الوقائية التي يمكن أن تحمي الأفراد والمجتمع الرقمي.

وتأتي هذه الدراسة لتسهم في تعزيز الوعي الرقمي، ودعم جهود المنصات الرقمية والحكومات، وتقديم إطار معرفي متكامل يمكن الاعتماد عليه في تصميم سياسات حماية ووقاية فعالة، تسهم في تقليل المخاطر الناتجة عن النصب الإلكتروني، وتعزيز أمن وخصوصية المستخدمين في الفضاء الرقمي.

### 1.1 مشكلة الدراسة

على الرغم من التطور الكبير في تقنيات المنصات الرقمية وتعدد وسائل الحماية، لا يزال النصب الإلكتروني يمثل تهديدًا متزايدًا لمستخدمي الإنترنت. ويعود السبب الأساسي في ذلك إلى أن المحتالين يعتمدون غالبًا على الهندسة الاجتماعية لاستغلال ضعف الوعي الرقمي لدى الأفراد، أكثر من الاعتماد على الاختراقات التقنية المعقدة.

وتتجلى المشكلة في أن المستخدمين العاديين، حتى من ذوي الخبرة التقنية المتوسطة، قد يقعون ضحايا للنصب الإلكتروني بسبب:

- الاستعجال في التعامل مع الرسائل أو الروابط غير الموثوقة.
- مشاركة معلومات شخصية أو رموز تحقق دون تحقق من مصدرها.
- الانخداع بعروض مغرية أو حسابات مزيفة تبدو موثوقة.

وتؤدي هذه الظاهرة إلى آثار متعددة تشمل خسائر مالية، انتهاك الخصوصية، تآكل الثقة بين المستخدمين، وحتى آثار نفسية واجتماعية على الضحايا، الأمر الذي يجعل من دراسة النصب الإلكتروني قضية ملحة على المستويين الأكاديمي والعملي.

## 1.2 أسئلة الدراسة

تسعى هذه الدراسة للإجابة عن الأسئلة الرئيسة التالية:

1. ما أشكال وأساليب النصب الإلكتروني الأكثر شيوعًا على المنصات الرقمية؟
2. ما العوامل النفسية والاجتماعية والتقنية التي تزيد من تعرض المستخدمين للنصب الإلكتروني؟
3. كيف يمكن للمستخدمين حماية أنفسهم بفعالية ضد النصب الإلكتروني؟
4. ما الدور الذي تلعبه المنصات الرقمية والقوانين الوطنية في الحد من هذه الظاهرة؟

## 1.3 فرضيات الدراسة

1. توجد فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني تبعًا للمستوى التعليمي للمستخدمين.
2. توجد فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني تبعًا للفئة العمرية.
3. توجد فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني تبعًا لمعدل الاستخدام اليومي للمنصات الرقمية.
4. تزداد مستويات التعرض للنصب الإلكتروني بزيادة معدل الاستخدام اليومي للمنصات الرقمية.
5. توجد فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني تبعًا لفعالة إستراتيجيات الوقاية والحماية الرقمية.

## 1.4 أهداف الدراسة

**الأهداف العامة:**

- تقديم دراسة شاملة للنصب الإلكتروني على المنصات الرقمية.
- تحليل أسبابه، أساليبه، وآثاره على المستخدمين والمجتمع.

**الأهداف الخاصة:**

1. تحديد أشكال وأساليب النصب الإلكتروني الأكثر شيوعًا.
2. دراسة العوامل النفسية والاجتماعية والتقنية التي تزيد من خطر التعرض للنصب.
3. تقييم الآثار الاقتصادية والاجتماعية والنفسية للنصب الإلكتروني على الأفراد.
4. اقتراح استراتيجيات الوقاية والتوعية الرقمية للحد من الظاهرة.

## 1.5 أهمية الدراسة

1. **أهمية علمية** :تسهم الدراسة في إثراء المعرفة الأكاديمية بمجال الجرائم الإلكترونية والوعي الرقمي، وتملأ فجوات الدراسة السابقة حول أساليب النصب الإلكتروني في المنصات الرقمية.
2. **أهمية عملية** :تساعد الجهات الحكومية والمنصات الرقمية والمؤسسات التعليمية في تصميم برامج توعية وحماية فعالة للمستخدمين.

3. **أهمية اجتماعية** :تعزيز الوعي الرقمي يحمي المجتمع من الخسائر المالية والنفسية والاجتماعية المرتبطة بالنصب الإلكتروني، ويعزز الثقة في الخدمات الرقمية.
4. **أهمية مستقبلية** :يوفر الدراسة إطارًا يمكن استخدامه لتطوير سياسات أمان وخصوصية رقمية ولائية وقومية، ودعم جهود مكافحة الجرائم الإلكترونية.

## 1.6 منهجية الدراسة

– تعتمد هذه الدراسة على المنهج الوصفي التحليلي لجمع وتحليل المعلومات المتعلقة بالنصب الإلكتروني على المنصات الرقمية.

– تم استخدام مقياس ليكرت الخماسي بصيغة التكرار **(دائمًا – غالبًا – أحيانًا – نادرًا – لا يحدث إطلاقًا)** لقياس مدى حدوث السلوك أو الظاهرة محل الدراسة، حيث يعكس زيادة التكرار ارتفاع مستوى الوعي أو شدة الأثر أو فعالية الاستراتيجيات الوقائية.

## 1.7 حدود الدراسة

تُحدَّد حدود هذه الدراسة في إطارها العلمي والمنهجي وفق المحاور الآتية:

### أولًا: الحدود الموضوعية

تقتصر هذه الدراسة على تناول **ظاهرة النصب الإلكتروني عبر المنصات الرقمية**، مع التركيز على أساليبه الشائعة مثل التصيّد الاحتيالي، الروابط المزيفة، الحسابات الوهمية، والابتزاز الرقمي، إضافة إلى دراسة العوامل النفسية والاجتماعية المؤدية لانتشاره، وآثاره الاقتصادية والاجتماعية والنفسية، واستراتيجيات الوقاية والحماية الرقمية. ولا تتناول الدراسة الجرائم الإلكترونية المتقدمة التي تعتمد على اختراقات تقنية معقدة أو هجمات سيبرانية متطورة موجهة للبنى التحتية.

### ثانيًا: الحدود المكانية

تُجرى هذه الدراسة في السياق السوداني، مع الأخذ في الاعتبار الخصائص الاجتماعية والثقافية والقانونية للمجتمع، ولا سيما في ظل تطبيق قانون جرائم المعلوماتية .وعليه، فإن نتائج الدراسة تُفسَّر ضمن هذا الإطار المكاني، مع إمكانية الاستفادة منها في سياقات عربية مشابهة مع مراعاة الفروق الثقافية والقانونية والتقنية.

### ثالثًا: الحدود الزمانية

تغطي الدراسة الفترة الزمنية الممتدة من **عام 2023م إلى عام 2025م**، وهي فترة شهدت تصاعدًا ملحوظًا في استخدام المنصات الرقمية وتزايدًا في معدلات النصب الإلكتروني، مما يجعلها إطارًا زمنيًا مناسبًا لرصد الظاهرة وتحليلها.

### رابعًا: الحدود البشرية

تقتصر الدراسة على مستخدمي المنصات الرقمية من البالغين الذين يستخدمون وسائل التواصل الاجتماعي والتطبيقات الرقمية بشكل منتظم، ممن وافقوا على المشاركة في الاستبيان. ولا تشمل الدراسة فئات الأطفال أو المستخدمين غير النشطين رقميًا.

### خامسًا: الحدود المنهجية

تعتمد الدراسة على **المنهج الوصفي التحليلي**، باستخدام الاستبانة كأداة رئيسية لجمع البيانات، وهو ما قد يحد من تعميم النتائج بسبب اعتمادها على البيانات الذاتية للمبحوثين، واحتمالية التحيز في الاستجابة أو عدم الدقة في الإفصاح.

## ثانياً: الدراسات السابقة

1. **Pitchan et al. (2025) – Cyber Fraud and Digital Awareness**

تناولت هذه الدراسة أكثر من 40 بحثًا حول النصب الإلكتروني عبر الإنترنت، مع التركيز على دور الثقافة الرقمية والوعي في الحد من تعرض المستخدمين للاحتيال الرقمي. استخدمت الدراسة المنهج المراجعة المنهجية لتحليل نتائج البحوث السابقة وتصنيف أشكال النصب وأساليبه. خلصت الدراسة إلى أن زيادة الوعي الرقمي والتثقيف المستمر للمستخدمين يقلل بشكل كبير من فرص الوقوع ضحايا النصب الإلكتروني، وأن العوامل النفسية والاجتماعية تلعب دورًا محوريًا في سهولة تعرض المستخدمين. ومن أبرز توصياتها تعزيز برامج التوعية الرقمية، وتدريب المستخدمين على التعرف على الروابط والحسابات المشبوهة، وتطبيق إجراءات وقائية فعّالة على المنصات الرقمية.

2. **Mouncey & Ciobotaru (2025) – Phishing Awareness on Social Media**

ركزت هذه الدراسة على تأثير التدريب حول التصيّد الاحتيالي (Phishing) على مستخدمي منصات التواصل الاجتماعي مثل .Instagram استخدمت الدراسة المنهج التجريبي، حيث تم تقسيم المشاركين إلى مجموعات متدربة وغير متدربة لمقارنة نتائج الوعي الرقمي والاستجابة للروابط الاحتيالية. خلصت الدراسة إلى أن التدريب الرقمي يزيد من وعي المستخدمين ويقلل من احتمالية الانخداع بالرسائل والروابط المزيفة، حتى بين المستخدمين ذوي الخبرة التقنية المتوسطة. ومن أبرز توصيات الدراسة إدماج برامج التوعية ضمن الاستخدام اليومي للمنصات الرقمية وتكرار التدريب بشكل دوري لتعزيز الفاعلية الوقائية.

3. **عوض (2025) – النصب الإلكتروني في العصر الرقمي**

تناولت هذه الدراسة مخاطر النصب الإلكتروني على المعاملات المالية وأساليب الاحتيال الشائعة مثل عروض العمل الوهمية والرسائل البنكية المزيفة، مع التركيز على السياق الرقمي العربي. واستخدمت الدراسة المنهج الوصفي التحليلي لجمع البيانات من حالات فعلية وتحليلها. خلصت الدراسة إلى أن ضعف الوعي الرقمي يعد العامل الأبرز في سقوط المستخدمين ضحايا الاحتيال، وأن وسائل الحماية الحالية على المنصات غير كافية

بشكل كامل .ومن أبرز توصياتها تطوير برامج توعية مستمرة للمستخدمين وإعادة تصميم سياسات الأمان للمنصات الرقمية لتقليل فرص الاحتيال.

4. **الاتجاهات الحديثة في الجرائم الإلكترونية عبر مواقع التواصل (دراسة عربية)**

ركزت هذه الدراسة على تطور أساليب الاحتيال الرقمي والنصب على منصات التواصل الاجتماعي في السياقات العربية، مع تحليل توجهات الباحثين في مجال الجرائم الإلكترونية. واستخدمت المنهج التحليلي والمراجعة الأدبية لتحديد الأساليب الحديثة والتقنيات المستخدمة من قبل المحتالين. خلصت الدراسة إلى أن ظاهرة النصب الرقمي تتزايد مع التحول الرقمي، وأن هناك فجوة معرفية واضحة لدى المستخدمين العرب فيما يخص الوقاية الرقمية .ومن أبرز توصيات الدراسة التركيز على التعليم الرقمي ضمن المناهج الدراسية وبرامج التوعية المجتمعية لتقليل المخاطر.

5. **Pew Research Center (2025) – Online Scams and Attacks in America Today**

استقصت هذه الدراسة مدى تعرض البالغين في الولايات المتحدة للنصب الإلكتروني وخسائرهم المالية نتيجة الرسائل الاحتيالية والروابط المزيفة على الإنترنت. واستخدمت الدراسة المنهج الاستقصائي لجمع بيانات من آلاف المشاركين عبر استبيانات منظمة. خلصت الدراسة إلى أن حوالي 20% من البالغين قد خسروا أموالًا بسبب النصب الإلكتروني، وأن ضعف التوعية الرقمية يرفع من احتمالات التعرض للغش الإلكتروني .ومن أبرز توصيات الدراسة تعزيز برامج التثقيف الرقمي، وتوفير أدوات أمان قوية للمستخدمين، ورفع الوعي بأساليب الاحتيال الحديثة.

6. **Acharya et al. (2024) – Fraudulent Donation Scams on Social Media**

تناولت هذه الدراسة عمليات الاحتيال المتعلقة بالتبرعات الوهمية على منصات Facebook و Instagram و Telegram ، مع التركيز على أساليب المحتالين في استغلال الحسابات المتعددة لإيهام المستخدمين بأن التبرعات حقيقية. واستخدمت الدراسة تحليل المحتوى الرقمي لفحص الرسائل والمنشورات الاحتيالية. خلصت الدراسة إلى أن المحتالين يبتكرون أساليب جديدة بشكل مستمر، وأن المنصات لا تكشف جميع العمليات الاحتيالية بشكل فعال .ومن أبرز توصياتها تعزيز المراقبة على المنصات، وتطبيق خوارزميات للكشف المبكر عن الحسابات الاحتيالية، وتوفير آليات تبليغ سهلة للمستخدمين.

7. **المسؤولية الجزائية عن جرائم النصب والاحتيال الإلكتروني في الجزائر**

ركزت هذه الدراسة على التشريعات الجزائرية المتعلقة بالنصب الإلكتروني ومسؤولية مرتكبي الجرائم الإلكترونية، وتحليل الثغرات القانونية في مواجهة الأساليب الحديثة. واستخدمت المنهج التحليلي القانوني لدراسة التشريعات ومقارنتها مع الممارسات العملية. خلصت الدراسة إلى أن هناك ثغرات تشريعية تحد من القدرة على مكافحة الجرائم الإلكترونية بفعالية، مع تفاوت في تطبيق القانون على المنصات الرقمية .ومن

أبرز توصياتها تحديث التشريعات الرقمية، وتوفير آليات قانونية فعالة لمعاقبة المحتالين الإلكترونيين، وتعزيز التعاون بين الجهات القضائية والمنصات.

8. **آليات القانونية لمكافحة الاحتيال عبر مواقع التواصل الاجتماعي (دراسة عربية)**

تناولت هذه الدراسة تحليل الآليات القانونية لمكافحة النصب الإلكتروني في المجتمعات العربية، مع التركيز على القوانين واللوائح الوطنية المرتبطة بالفضاء الرقمي. واستخدمت المنهج الوصفي التحليلي القانوني لدراسة نصوص القوانين وتحليل فعاليتها. خلصت الدراسة إلى أن ضعف الأطر التشريعية الحالية وعدم مواكبتها للتطور الرقمي يقلل من فعالية مكافحة الاحتيال الإلكتروني .ومن أبرز توصياتها تعديل القوانين بما يتوافق مع التطور التكنولوجي، وزيادة التعاون بين الجهات الرقابية والمنصات الرقمية، وتعزيز وعي المستخدمين بحقوقهم.

9. **التقرير الحكومي السعودي عن الاحتيال الرقمي (2023)**

ركز هذا التقرير على توثيق تطور الاحتيال الإلكتروني وأساليبه في المملكة العربية السعودية، مع استعراض الأمثلة والتحديات التي تواجه الجهات الرسمية في التصدي للظاهرة. واستخدم التقرير تحليل بيانات وتقارير رسمية .خلص التقرير إلى أن التحول الرقمي وزيادة استخدام منصات التواصل أديا إلى ارتفاع التعرض للنصب الإلكتروني، خصوصًا بين المستخدمين غير الواعيين رقميًا .ومن أبرز توصيات التقرير تعزيز برامج التوعية الرقمية، وتطوير أدوات حماية المستخدمين، وفرض آليات رقابية أفضل على المنصات.

10. **Early Research on Phishing and Cognitive Factors (PMC, 2020)**

ركزت هذه الدراسة على تأثير العوامل النفسية والمعرفية على تعرض المستخدمين للتصيّد الإلكتروني عبر مواقع التواصل الاجتماعي. واستخدمت المنهج التجريبي التحليلي، حيث تم دراسة سلوك المستخدمين وأنماط التعاطي مع الرسائل الاحتيالية. خلصت الدراسة إلى أن الخصائص السلوكية والمعرفية للمستخدمين تلعب دورًا حاسمًا في احتمالية الوقوع ضحية النصب الإلكتروني .ومن أبرز توصياتها تصميم برامج تدريبية تتوافق مع الأنماط المعرفية المختلفة للمستخدمين لتعزيز الوعي الرقمي وتقليل فرص التعرض للنصب.

**أوجه الاتفاق والاختلاف بين هذه الدراسة والدراسات السابقة:**

تتفق الدراسة الحالية مع الدراسات السابقة على عدة نقاط رئيسية، أبرزها تأكيد أهمية الوعي الرقمي في الحد من التعرض للنصب الإلكتروني، وتعدد أساليب الاحتيال الرقمي، إضافة إلى الدور النفسي والاجتماعي للمستخدمين في سهولة الوقوع كضحايا، وضرورة تبني إجراءات وقائية وتوعوية فعّالة. كما تتفق الدراسة مع الدراسات العربية والأجنبية في الإشارة إلى تأثير العوامل السلوكية والمعرفية على احتمالية التعرض للنصب، وإبراز أهمية برامج التدريب والتثقيف الرقمي، وتحديث التشريعات الوطنية لتعزيز الأمن السيبراني.

من جهة أخرى، تميزت الدراسة الحالية بعدة أوجه اختلاف عن الدراسات السابقة، أبرزها التركيز على السياق السوداني، ومراعاة الخصائص الاجتماعية والثقافية للمستخدمين المحليين، بالإضافة إلى شمولية المنصات الرقمية بحيث تشمل جميع منصات التواصل والتطبيقات التجارية والدفع الإلكتروني، بدل التركيز على منصة

واحدة فقط كما في بعض الدراسات الأجنبية. كما تقدم الدراسة تحليلًا متعدد الأبعاد يجمع بين الجانب التقني والاجتماعي والاقتصادي، مع اقتراح توصيات عملية قابلة للتطبيق لتعزيز الوقاية الرقمية لدى المستخدمين والمنصات والحكومات، ما يمنحها قيمة علمية وعملية أكبر مقارنة ببعض الدراسات السابقة التي اقتصرت على التحليل النظري أو الإطار القانوني فقط.

## 2. الإطار المفاهيمي والنظري للدراسة:

يمثل الإطار المفاهيمي حجر الزاوية في أي دراسة علمية، حيث يوفر الأساس النظري والمفاهيمي لفهم الظاهرة محل البحث ويحدد المفاهيم والمصطلحات الرئيسة والعلاقات بينها. في هذه الدراسة، يهدف الإطار المفاهيمي إلى توضيح طبيعة النصب الإلكتروني على المنصات الرقمية، وأساليبه، والعوامل المؤثرة فيه، وآثاره على الأفراد والمجتمع الرقمي، مع التركيز على البنية المعرفية والسلوكية للمستخدمين.

يعتمد الإطار المفاهيمي على تحديد المفاهيم الأساسية مثل النصب الإلكتروني، الاحتيال الرقمي، الهندسة الاجتماعية، الخصوصية الرقمية، والوعي الرقمي، مع شرح كيفية ترابط هذه المفاهيم في سياق المنصات الرقمية. كما يسعى إلى بناء تصور متكامل يربط بين الأسباب والنتائج والآثار الوقائية، بحيث يشكل قاعدة معرفية لتفسير الظاهرة ودراسة العلاقة بين العوامل التقنية والاجتماعية والسلوكية، ويتيح توجيه البحث نحو استنتاج توصيات عملية فعّالة للحد من النصب الإلكتروني.

**بناءً على هذا المدخل، سيُفصل الإطار المفاهيمي في أقسام فرعية تشمل:**

1. النصب الإلكتروني وأنواعه على المنصات الرقمية.
2. الهندسة الاجتماعية ودورها في الاحتيال الرقمي.
3. الآثار الاقتصادية والاجتماعية والنفسية للنصب الإلكتروني.
4. الأمن السيبراني وأدوات الحماية الرقمية.
5. التوعية الرقمية والوقاية من النصب الإلكتروني.

يُسهم هذا الإطار في توفير رؤية شاملة ومنهجية لفهم الظاهرة، ويضع أسسًا واضحة لربط الدراسات السابقة بالممارسات الواقعية، مع تعزيز قدرة الباحث على تفسير النتائج وتقديم توصيات قابلة للتطبيق على المستوى الفردي والمؤسسي.

### 2.1 مصطلحات الدراسة:

#### 1. الفضاء الرقمي(Digital Space)

الفضاء الرقمي هو البيئة الإلكترونية التي تشمل جميع المنصات والخدمات الرقمية، بما في ذلك الإنترنت، الشبكات الاجتماعية، تطبيقات الهواتف الذكية، البريد الإلكتروني، والتفاعلات الرقمية بين الأفراد والمؤسسات. يشكل الفضاء الرقمي الإطار العام الذي تحدث فيه جميع الأنشطة الرقمية، بما في ذلك التجارة الإلكترونية، التواصل الاجتماعي، والتعليم عن بعد، ويُعتبر البيئة التي تتكشف فيها جرائم النصب الإلكتروني

والاحتيال الرقمي(2001) .Castells, M **مثال** :استخدام منصات مثل واتساب وفيسبوك للشراء والبيع والتواصل الاجتماعي ضمن الفضاء الرقمي.

### 2. النصب الإلكتروني(Cyber Fraud)

النصب الإلكتروني هو عملية احتيال تتم عبر الإنترنت بهدف الحصول على أموال أو بيانات شخصية أو معلومات حساسة بطريقة خادعة. يتميز هذا النوع من الاحتيال بسرعة الانتشار وإمكانية استهداف عدد كبير من المستخدمين في وقت قصير، وغالبًا ما يتم عبر رسائل البريد الإلكتروني المزيفة، الروابط الوهمية، أو الحسابات الوهمية على منصات التواصل الاجتماعي. ويعد النصب الإلكتروني خطيرًا لأنه لا يؤدي فقط إلى خسائر مالية، بل يمكن أن يتسبب في سرقة الهوية، فقدان الخصوصية، والإضرار بالثقة بين الأفراد والمؤسسات(2007) .Wall, D. S .

### 3. الاحتيال الرقمي(Digital Scam)

الاحتيال الرقمي يشير إلى كل أساليب الغش والخداع التي يتم تنفيذها عبر الوسائل الرقمية بغرض تحقيق مكاسب غير مشروعة. يختلف عن النصب الإلكتروني في أنه قد يشمل مجموعة واسعة من العمليات الاحتيالية الرقمية، بما في ذلك الاحتيال المالي، الاحتيال على الهوية، والتلاعب بالمعلومات على المنصات الرقمية. ويتميز الاحتيال الرقمي بسهولة التكرار، وقدرته على الوصول إلى المستخدمين عبر التطبيقات، المواقع، أو البريد الإلكتروني دون الحاجة لتفاعل مباشر.(2019).Choi, et al .

### 4. التصيّد الاحتيالي(Phishing)

التصيّد الاحتيالي هو شكل من أشكال الاحتيال الرقمي الذي يعتمد على إرسال رسائل أو روابط مزيفة تبدو رسمية بهدف خداع المستخدمين للكشف عن بياناتهم الشخصية أو المالية. يشمل التصيّد الاحتيالي رسائل البريد الإلكتروني، الرسائل النصية، أو الرسائل المباشرة على منصات التواصل الاجتماعي. ويعد هذا الأسلوب من أكثر الأساليب شيوعًا على الإنترنت نظرًا لسهولة تنفيذه وفعاليته العالية في استهداف المستخدمين غير الواعيين.(2007) .Jakobsson,et al

### 5. الروابط المزيفة(Phishing Links)

الروابط المزيفة هي روابط إلكترونية تبدو شرعية للمستخدم لكنها في الواقع تؤدي إلى مواقع مزيفة تهدف إلى سرقة معلوماته الشخصية أو تحميل برمجيات خبيثة على جهازه. غالبًا ما تستخدم هذه الروابط في رسائل البريد الإلكتروني أو الرسائل النصية أو منشورات منصات التواصل الاجتماعي لإيهام المستخدم بأنها من مصدر موثوق، مما يجعل الضحية ينقر عليها ويكشف بياناته أو يُصاب بالبرمجيات الضارة. **مثال** : رسالة بريد إلكتروني تبدو وكأنها من بنك المستخدم وتحتوي على رابط لتحديث بيانات الحساب، وعند النقر عليها تُوجه المستخدم إلى موقع مزيف يقوم بسرقة بياناته المصرفية.(2007) .Abu-Nimeh, et al.

### 6. الحسابات الوهمية(Fake Accounts)

الحسابات الوهمية هي حسابات على المنصات الرقمية تُنشأ باسم شخص أو جهة مزيفة بغرض الاحتيال أو التضليل. يستخدم المحتالون هذه الحسابات لتقليد شخصيات حقيقية، إنشاء هوية زائفة، أو نشر محتوى

احتيالي لإقناع المستخدمين بالتفاعل معهم أو تقديم معلومات حساسة. وتُعد الحسابات الوهمية من أكثر أدوات الاحتيال الرقمي انتشارًا على منصات التواصل الاجتماعي. **مثال** :حساب على فيسبوك باسم شركة مشهورة يرسل عروضًا وهمية للحصول على بيانات الدفع الخاصة بالمستخدمين .(2010) .Stringhini, et al

### 7. الأمن السيبراني(Cybersecurity)

الأمن السيبراني يشمل جميع الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة الرقمية، البيانات، والشبكات من الهجمات الإلكترونية أو الاحتيال الرقمي. ويشـــمل ذلك برامج الحماية، جدران الحماية، تحديث الأنظمة، وإدارة كلمات المرور والمصادقة الثنائية. يلعب الأمن السيبراني دورًا أساسيًا في حماية المستخدمين والشركات من الخسائر المالية والمعلوماتية الناتجة عن النصب الإلكتروني .(2015) .Schneier, B

### 8. الوقاية الرقمية(Digital Prevention)

الوقاية الرقمية هي الإجراءات الاستباقية التي تهدف إلى الحد من خطر التعرض للنصب الإلكتروني، وتشمل الجانب التوعوي، التقني، والتنظيمي. يشمل ذلك برامج التوعية والتدريب، استخدام أدوات الكشف عن الحسابات المزيفة أو الروابط المشبوهة، تطبيق سياسات الأمان على المنصات، وتثقيف المستخدمين حول سلوكيات الأمان الرقمي. تساعد الوقاية الرقمية على حماية الأفراد والمؤسسات من الخسائر المالية والنفسية والاجتماعية الناتجة عن النصب الإلكتروني. (2018) .Hadnagy, C

### 9. الهندسة الاجتماعية(Social Engineering)

الهندسة الاجتماعية هي مجموعة من الأساليب الاحتيالية التي تعتمد على استغلال السلوك البشري بدلاً من استغلال الثغرات التقنية. يركز المحتالون على الجوانب النفسية والاجتماعية للمستخدمين، مثل الثقة، الطمع، أو الخوف، لإقناعهم بالكشـــف عن معلوماتهم الشـــخصـــية أو القيام بأفعال تهدد أمنهم الرقمي. تعد الهندســـة الاجتماعية أحد أكثر أساليب الاحتيال فاعلية لأنها تستغل الطبيعة البشرية المباشرة، مما يجعلها تشكل تهديدًا كبيرًا حتى للأشخاص ذوي الخبرة التقنية(2011) .Mitnick, et al .

### 10.الوعي الرقمي(Digital Awareness)

الوعي الرقمي هو القدرة على إدراك المخاطر الرقمية وفهم ســـلوكيات الأمان المطلوبة عند اســـتخدام الإنترنت والمنصات الرقمية. يشمل ذلك معرفة أساليب الاحتيال، القدرة على التحقق من صحة الروابط والحسابات، وعدم مشاركة معلومات حساسة إلا مع مصادر موثوقة. يعد الوعي الرقمي من أهم الأدوات الوقائية ضد النصب الإلكتروني، حيث يقلل من احتمالية وقوع المستخدم ضحية للهجمات الرقمية حتى عند مواجهة محتوى احتيالي متقن. (2014) .Arachchilage, et al

### 11.الخصوصية الرقمية(Digital Privacy)

الخصوصية الرقمية تعني حماية المعلومات والبيانات الشخصية للمستخدمين على الإنترنت من الوصول غير المصـــرح به أو الاســـتغلال غير القانوني. تشـــمل هذه الخصـــوصـــية البيانات المالية، معلومات الحســـابات،

والمراسلات الرقمية. الحفاظ على الخصوصية الرقمية يمنع الانتهاكات ويقلل من احتمالية التعرض للنصب والاحتيال، كما يعزز ثقة المستخدمين في المنصات الرقمية والخدمات الإلكترونية(2008) .Solove, D. J .

### 12.البيانات الشخصية(Personal Data)

البيانات الشخصية هي أي معلومات تحدد هوية المستخدم أو تساعد على التعرف عليه، مثل الاسم، البريد الإلكتروني، رقم الهاتف، أو الموقع الجغرافي. تُعتبر البيانات الشخصية هدفًا رئيسيًا للمحتالين الرقميين لأنها يمكن استخدامها للسرقة، الاحتيال المالي، أو ابتزاز الأفراد. حماية هذه البيانات تعد جزءًا أساسيًا من الخصوصية الرقمية والأمن السيبراني.**مثال** :تسريب بيانات المستخدمين من أحد مواقع التسوق الإلكتروني يؤدي إلى استهدافهم برسائل احتيالية. (2016) .GDPR

### 13.الابتزاز الرقمي(Cyber Extortion)

الابتزاز الرقمي هو استخدام البيانات أو الصور أو المعلومات الشخصية للضغط على الأفراد أو المؤسسات للحصول على مكاسب مالية أو مطالب أخرى غير مشروعة. يعتمد هذا النوع من الجرائم على تهديد الضحية بنشر المعلومات أو تعطيل الخدمات الرقمية إذا لم يتم الامتثال للمطالب. ويعد الابتزاز الرقمي أحد أخطر أشكال الجرائم الإلكترونية لأنه يجمع بين التهديد النفسي والخسائر المالية. **مثال** :مهاجم يحصل على صور شخصية للضحية ويهدد بنشرها على الإنترنت ما لم يُدفع مبلغ مالي معين. (2012) .Moore, et al

### 14.الجرائم الإلكترونية(Cyber Crimes)

الجرائم الإلكترونية هي كل الأعمال المخالفة للقانون التي تُنفذ باستخدام الإنترنت أو التكنولوجيا الرقمية بهدف الإضرار بالأفراد أو المؤسسات، وتشمل الاحتيال الرقمي، النصب الإلكتروني، الابتزاز الرقمي، اختراق الأنظمة، والتجسس على البيانات. تعتبر الجرائم الإلكترونية من أخطر التهديدات في العصر الرقمي، لما لها من آثار مالية، اجتماعية، ونفسية على الضحايا. (2007) .Wall, D. S **مثال** : مجموعة تقوم باختراق بيانات شركة للحصول على معلومات حساسة وبيعها على الشبكة السوداء.

### 2.2 العوامل النفسية والاجتماعية المؤدية للنصب الإلكتروني:

تُعد العوامل النفسية والاجتماعية من أبرز المحددات التي تفسّر قابلية الأفراد للوقوع ضحية لعمليات النصب الإلكتروني، إذ يستغل المحتالون نقاط الضعف الإنسانية والظروف الاجتماعية لتحقيق أهدافهم الاحتيالية.

**أولًا: ضعف الوعي والثقافة الرقمية**

يُعد ضعف الوعي الرقمي من أهم العوامل النفسية التي تسهم في تعرض الأفراد للنصب الإلكتروني، حيث يفتقر كثير من المستخدمين إلى المعرفة بأساليب الاحتيال الحديثة، مثل التصيد الاحتيالي والروابط المزيفة والحسابات الوهمية. هذا القصور المعرفي يجعل الفرد أقل قدرة على التمييز بين المحتوى الحقيقي والمحتوى الاحتيالي، وأكثر عرضة للخداع (العنزي، 2020).

**ثانيًا: الثقة الزائدة وسهولة التأثير**

يميل بعض الأفراد إلى إظهار قدر عالٍ من الثقة بالآخرين في الفضاء الرقمي، خاصة عندما يتم تقديم المحتال في صورة جهة رسمية أو شخصية موثوقة. وتُعد هذه الثقة الزائدة عاملًا نفسيًا رئيسيًا يستغله المحتالون، لا سيما في المجتمعات التي تتسم بالعلاقات الاجتماعية القائمة على حسن النية (الزهراني، 2021).

**ثالثًا: الطمع والرغبة في الربح السريع**

يستغل المحتالون النزعة النفسية لدى بعض الأفراد في تحقيق مكاسب مالية سريعة دون مجهود، من خلال الإعلانات الوهمية، والجوائز المزيفة، وفرص الاستثمار الكاذبة. وتؤكد الدراسات أن الطمع يُضعف التفكير النقدي ويجعل الفرد أكثر قابلية لاتخاذ قرارات غير مدروسة (الحميدي، 2019).

**رابعًا: الخوف والضغط النفسي**

يُستخدم الخوف كأداة نفسية فعّالة في عمليات النصب الإلكتروني، مثل التهديد بإيقاف الحسابات أو الادعاء بوجود مخالفات قانونية. وتحت تأثير القلق والضغط النفسي، يتخذ الضحايا قرارات سريعة دون التحقق من صحة المعلومات، مما يزيد من احتمالية الوقوع في الاحتيال (القحطاني، 2022).

**خامسًا: العزلة الاجتماعية وضعف الدعم الأسري**

تشير بعض الدراسات إلى أن الأفراد الذين يعانون من العزلة الاجتماعية أو ضعف الروابط الأسرية يكونون أكثر عرضة للنصب الإلكتروني، حيث يبحثون عن التفاعل أو الدعم عبر المنصات الرقمية، وهو ما يستغله المحتالون لبناء علاقات زائفة تمهيدًا للاحتيال (السلمي، 2020).

**سادسًا: الظروف الاقتصادية والاجتماعية**

تلعب الظروف الاقتصادية الصعبة، مثل البطالة وضعف الدخل، دورًا اجتماعيًا مهمًا في زيادة معدلات النصب الإلكتروني، إذ تدفع هذه الظروف بعض الأفراد إلى البحث عن حلول سريعة، مما يجعلهم فريسة سهلة لعمليات الاحتيال الرقمي (عبدالله، 2021).

## 2.3 آثار الجرائم الإلكترونية على الأفراد والمجتمع:

أصبحت الجرائم الإلكترونية من أخطر التحديات التي تواجه المجتمعات المعاصرة، لما تخلّفه من آثار متعددة تمس الفرد والمجتمع على حد سواء، وتمتد آثارها إلى الجوانب النفسية والاقتصادية والاجتماعية والأمنية.

### أولًا: الآثار النفسية على الأفراد

تُخلّف الجرائم الإلكترونية آثارًا نفسية عميقة لدى الضحايا، أبرزها القلق والخوف المستمر وفقدان الشعور بالأمان الرقمي، خاصة في حالات الابتزاز الإلكتروني وانتهاك الخصوصية. وقد يعاني الضحايا من الاكتئاب، وتراجع الثقة بالآخرين، والعزلة الاجتماعية نتيجة الصدمة النفسية المرتبطة بتجربة الاحتيال أو التشهير الرقمي (القحطاني، 2022).

### ثانيًا: الآثار الاقتصادية والمالية

تتمثل الآثار الاقتصادية في الخسائر المالية المباشرة التي يتعرض لها الأفراد والمؤسسات نتيجة عمليات النصب والاحتيال الإلكتروني وسرقة البيانات البنكية. كما تؤدي هذه الجرائم إلى استنزاف الموارد الاقتصادية للمجتمع، وزيادة تكاليف الحماية الرقمية، وتعطيل الأنشطة التجارية الإلكترونية (عبدالله، 2021).

**ثالثًا: انتهاك الخصوصية والهوية الرقمية**

تؤدي الجرائم الإلكترونية إلى انتهاك الخصوصية الشخصية وسرقة الهوية الرقمية، من خلال الاستيلاء على البيانات الشخصية أو استغلالها دون إذن. ويُعد هذا الأثر من أخطر الآثار، لما يترتب عليه من استخدام غير مشروع للبيانات في الابتزاز أو التشهير أو ارتكاب جرائم أخرى باسم الضحية (العنزي، 2020).

**رابعًا: تراجع الثقة في الفضاء الرقمي**

يسهم انتشار الجرائم الإلكترونية في إضعاف ثقة الأفراد والمجتمع في المنصات الرقمية والخدمات الإلكترونية، مما يحد من الاستفادة من التحول الرقمي والحكومة الإلكترونية والتجارة الإلكترونية. كما يؤدي ذلك إلى عزوف بعض الفئات عن استخدام التقنيات الحديثة خوفًا من التعرض للاحتيال (الزهراني، 2021).

**خامسًا: الآثار الاجتماعية والأسرية**

تنعكس الجرائم الإلكترونية سلبًا على العلاقات الاجتماعية والأسرية، خاصة في حالات الابتزاز أو التشهير، حيث قد يتعرض الضحية للنبذ الاجتماعي أو فقدان السمعة، مما يؤثر على استقرار الأسرة وتماسكها. كما تسهم هذه الجرائم في نشر السلوكيات السلبية داخل المجتمع، مثل الخداع وانعدام الثقة (السلمي، 2020).

**سادسًا: الآثار الأمنية والمجتمعية العامة**

على المستوى المجتمعي، تشكل الجرائم الإلكترونية تهديدًا للأمن المجتمعي والرقمي، إذ قد تُستخدم في تمويل أنشطة غير مشروعة أو زعزعة الاستقرار الاجتماعي. كما تُثقل كاهل الأجهزة الأمنية والقضائية، وتتطلب تطوير تشريعات وسياسات خاصة لمواجهتها (الحميدي، 2019).

## 2.3 استراتيجيات الحماية والوقاية الرقمية:

تمثل الحماية والوقاية الرقمية ركيزة أساسية للحد من الجرائم الإلكترونية وتقليل آثارها على الأفراد والمجتمع، حيث تعتمد هذه الاستراتيجيات على مزيج من الوعي البشري، والتقنيات الأمنية، والأطر التشريعية والتنظيمية.

**أولًا: تعزيز الوعي والثقافة الرقمية**

يُعد رفع مستوى الوعي الرقمي لدى المستخدمين من أهم استراتيجيات الوقاية، إذ يسهم في تمكين الأفراد من التعرف على أساليب الاحتيال الإلكتروني مثل التصيد الاحتيالي والروابط المزيفة والهندسة الاجتماعية. وتشير الدراسات إلى أن التدريب المستمر والتثقيف الرقمي يقللان بشكل ملحوظ من احتمالية وقوع المستخدم ضحية للهجمات الإلكترونية.(Whitman & Mattord, 2021)

**ثانيًا: استخدام أدوات وتقنيات الأمن السيبراني**

تشمل هذه الاستراتيجية الاعتماد على البرمجيات والتقنيات الوقائية، مثل برامج مكافحة الفيروسات، وجدران الحماية، وأنظمة كشف التسلل، وتحديث الأنظمة بانتظام. وتؤكد الأدبيات الأمنية أن استخدام أدوات الحماية المحدثة يقلل من فرص اختراق الأجهزة وسرقة البيانات الشخصية.(Stallings, 2020)

**ثالثًا: إدارة كلمات المرور والتحقق الثنائي**

تُعد كلمات المرور القوية واستخدام المصادقة الثنائية من أكثر الإجراءات فاعلية في حماية الحسابات الرقمية. إذ توصي الدراسات باستخدام كلمات مرور معقدة وفريدة لكل حساب، مع تفعيل التحقق الثنائي لتقليل مخاطر الاختراق حتى في حال تسرب بيانات الدخول.(Anderson, 2020)

**رابعًا: حماية البيانات والخصوصية الرقمية**

تشمل هذه الاستراتيجية الحد من مشاركة البيانات الشخصية، واستخدام إعدادات الخصوصية في المنصات الرقمية، وتشفير البيانات الحساسة. وتؤكد الأبحاث أن حماية الخصوصية الرقمية تسهم في تقليل جرائم سرقة الهوية والابتزاز الإلكتروني.(Solove & Schwartz, 2021)

**خامسًا: الإبلاغ المبكر والتعامل مع الحوادث الرقمية**

يُعد الإبلاغ السريع عن محاولات الاحتيال أو الاختراق عنصرًا أساسيًا في الوقاية الرقمية، حيث يساعد الجهات المختصة على تتبع الجناة والحد من انتشار الهجمات. وتشير الدراسات إلى أن نظم الاستجابة للحوادث تقلل من حجم الخسائر وتحد من تكرار الهجمات الإلكترونية.(NIST, 2018)

**سادسًا: دور التشريعات والسياسات الأمنية**

تلعب القوانين والتشريعات الرقمية دورًا محوريًا في الوقاية من الجرائم الإلكترونية، من خلال تجريم الأفعال الرقمية غير المشروعة، وفرض العقوبات الرادعة، وتنظيم حماية البيانات. وتؤكد الدراسات المقارنة أن وجود أطر قانونية واضحة يعزز الثقة في الفضاء الرقمي ويحد من السلوك الإجرامي.(Brenner, 2019)

## 2.4 قانون مكافحة جرائم المعلوماتية السوداني لسنة 7007 تعديل لسنة 2018م:

يُعد قانون جرائم المعلوماتية السوداني أحد أهم الأدوات التشريعية التي وضعتها الدولة لمواجهة التحديات المتزايدة المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات في ارتكاب الجرائم، وعلى رأسها النصب والاحتيال الإلكتروني، والابتزاز الرقمي، وانتهاك الخصوصية، وسرقة البيانات. ويهدف هذا القانون إلى تنظيم استخدام الوسائط الرقمية، وحماية الأفراد والمؤسسات من المخاطر الناشئة في الفضاء الرقمي، وضمان الاستخدام الآمن والمسؤول للتقنية.

ويُجرّم قانون جرائم المعلوماتية عددًا من الأفعال المرتبطة مباشرة بموضوع الدراسة، من بينها: الدخول غير المشروع إلى الأنظمة المعلوماتية، وانتحال الشخصية الرقمية، واستخدام الروابط المزيفة والحسابات الوهمية، والاحتيال الإلكتروني، والابتزاز باستخدام الوسائط الرقمية، إضافة إلى الاعتداء على البيانات الشخصية وسريتها. كما يحدد القانون العقوبات الرادعة التي تتراوح بين الغرامات المالية والعقوبات بالسجن التي تتراوح بين سنتين إلى عشر سنوات أو الأثنين معاً، تبعًا لجسامة الفعل وآثاره.

ويؤكد القانون على أهمية حماية البيانات الشخصية وعدم استخدامها أو نشرها دون موافقة أصحابها، وهو ما ينسجم مع البعد الوقائي للدراسة، حيث يسهم وجود إطار قانوني واضح في رفع مستوى الردع العام والخاص، وتعزيز ثقة المستخدمين في التعاملات الإلكترونية، والحد من انتشار جرائم النصب الإلكتروني.

كما يُبرز قانون جرائم المعلوماتية دور الجهات العدلية والتنفيذية في التحري والتحقيق في الجرائم الرقمية، ويُعطي الشرعية لاستخدام الأدلة الإلكترونية أمام المحاكم، وهو ما يعزز فعالية إنفاذ القانون في مواجهة الجرائم المستحدثة التي تعتمد على التقنيات الحديثة، **ويمثل إطارًا تشريعيًا ضروريًا لمواجهة الجرائم الرقمية، إلا أن فعاليته تظل مرهونة بـ:**

- **التحديث المستمر** ليشمل التطور المتسارع في أساليب النصب، مثل الاحتيال عبر العملات الرقمية أو الذكاء الاصطناعي.
- **تعزيز الجوانب الوقائية والتوعوية** مثل إلزام الجهات المعنية ببرامج توعية رقمية، أو تحميل المنصات الرقمية مسؤوليات واضحة في حماية المستخدمين والإبلاغ عن المحتوى الاحتيالي.
- **تطوير آليات التحقيق الرقمي** في إثبات الجرائم المعلوماتية، لا سيما ما يتعلق بجمع الأدلة الرقمية، وحفظها، والتحقق من سلامتها الفنية.
- **سن تشريع مكمّل خاص بحماية البيانات الشخصية** خاصة مع التوسع في استخدام المنصات الرقمية والخدمات الإلكترونية.

## 3. الدراسة الميدانية والنتائج والتوصيات:

يعرض هذا الجزء نتائج التحليل الإحصائي لبيانات الدراسة الميدانية التي تم جمعها من أفراد عينة البحث، وذلك باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية .(SPSS) وقد شمل التحليل الإحصاء الوصفي واختبارات الثبات والصدق، إضافة إلى اختبار فرضيات الدراسة باستخدام الأساليب الإحصائية الملائمة لطبيعة المتغيرات ومستوى قياسها، عند مستوى دلالة إحصائية.($\alpha \leq 0.05$)

وتُعرض النتائج في مجموعة من الجداول الإحصائية التي توضح الخصائص الديموغرافية لعينة الدراسة، والمتوسطات الحسابية والانحرافات المعيارية لمحاور الاستبيان، فضلًا عن نتائج اختبارات الارتباط والفروق والانحدار، بما يسهم في تفسير الظاهرة محل الدراسة، ومناقشة النتائج في ضوء أهداف الدراسة وفرضياتها والإطار النظري والدراسات السابقة.

### أولًا: الجداول الوصفية للبيانات الديموغرافية

**الجدول (1): التوزيع التكراري لعينة الدراسة حسب الجنس**

| النوع | التكرار | النسبة المئوية (%) |
|---|---|---|
| ذكر | 110 | 50.7 |
| أنثى | 107 | 49.3 |
| **الإجمالي** | **217** | **100** |

يوضح الجدول (1) التوزيع التكراري لعينة الدراسة حسب متغير الجنس، حيث بلغ إجمالي أفراد العينة (217) مفردة. وتشير النتائج إلى تقارب واضح في تمثيل الجنسين، إذ شكّل الذكور (110) مفردات بنسبة (50.7%)، في حين بلغ عدد الإناث (107) مفردات بنسبة (49.3%). ويعكس هذا التوازن النسبي بين الذكور والإناث تجانسًا مقبولًا في توزيع العينة، مما يسهم في تعزيز موضوعية النتائج وإمكانية تعميمها، كما يقلل من احتمالية تحيز النتائج لصالح أحد الجنسين عند تحليل الفروق أو العلاقات المرتبطة بمتغيرات الدراسة اللاحقة.

**الجدول (2): التوزيع التكراري لعينة الدراسة حسب الفئة العمرية**

| الفئة العمرية | التكرار | النسبة المئوية (%) |
|---|---|---|
| أقل من 20 سنة | 24 | 11.1 |
| من 21 إلى 30 سنة | 65 | 30.0 |
| من 31 إلى 40 سنة | 62 | 28.6 |
| أكثر من 40 سنة | 43 | 19.8 |
| من 41 فأكثر | 23 | 10.6 |
| **الإجمالي** | **217** | **100** |

يبين الجدول (2) التوزيع التكراري لعينة الدراسة حسب الفئة العمرية، حيث بلغ إجمالي حجم العينة (217) مفردة. وتشير النتائج إلى أن الفئة العمرية من (21–30) سنة جاءت في المرتبة الأولى من حيث التمثيل بنسبة (30.0%) وبعدد (65) مفردة، تلتها الفئة العمرية من (31–40) سنة بنسبة (28.6%) وبعدد (62) مفردة، وهو ما يعكس هيمنة الفئات العمرية الشابة والمتوسطة على عينة الدراسة. في المقابل، بلغت نسبة الأفراد الذين تقل أعمارهم عن 20 سنة (11.1%)، بينما توزعت الفئات العمرية الأكبر سنًا بين فئة أكثر من 40 سنة بنسبة (19.8%)، وفئة (41 فأكثر) بنسبة (10.6%). ويشير هذا التوزيع إلى تنوع عمري مناسب داخل العينة، مع تركّز نسبي في الفئات الأكثر استخدامًا للمنصات الرقمية، الأمر الذي يدعم ملاءمة العينة لأهداف الدراسة المتعلقة بالتعرض للنصب الإلكتروني وتحليل أنماط السلوك الرقمي عبر المراحل العمرية المختلفة.

**الجدول (3): التوزيع التكراري لعينة الدراسة حسب المستوى التعليمي**

| المستوى التعليمي | التكرار | النسبة المئوية (%) |
|---|---|---|
| ثانوي فأقل | 25 | 11.5 |
| دبلوم | 43 | 19.8 |
| بكالوريوس | 84 | 38.7 |
| دراسات عليا | 65 | 30.0 |
| **الإجمالي** | **217** | **100** |

يوضح الجدول (3) التوزيع التكراري لعينة الدراسة حسب المستوى التعليمي، حيث بلغ إجمالي أفراد العينة (217) مفردة. وتُظهر النتائج أن حملة درجة البكالوريوس يمثلون النسبة الأعلى من العينة بواقع (38.7%) وعدد (84) مفردة، يليهم حملة الدراسات العليا بنسبة (30.0%) وعدد (65) مفردة، وهو ما يشير إلى ارتفاع المستوى التعليمي العام لعينة الدراسة. في المقابل، بلغت نسبة ذوي المستوى التعليمي (ثانوي فأقل) (11.5%) بعدد (25) مفردة، بينما شكل حملة الدبلوم نسبة (19.8%) بعدد (43) مفردة. ويعكس هذا التوزيع تنوعًا تعليميًا مناسبًا داخل العينة، بما يسمح بتحليل الفروق في التعرض للنصب الإلكتروني ومستويات الوعي الرقمي باختلاف المستويات التعليمية، كما يعزز من موثوقية النتائج وإمكانية تعميمها ضمن إطار الدراسة.

**الجدول (4): التوزيع التكراري لعينة الدراسة حسب معدل الاستخدام اليومي للمنصات الرقمية**

| معدل الاستخدام اليومي للإنترنت | التكرار | النسبة المئوية (%) |
|---|---|---|
| أقل من ساعة | 44 | 20.3 |
| من 1 – 3 ساعات | 45 | 20.7 |
| من 4 – 6 ساعات | 44 | 20.3 |
| أكثر من 6 ساعات | 84 | 38.7 |
| **الإجمالي** | **217** | **100** |

يبين الجدول (4) التوزيع التكراري لعينة الدراسة حسب معدل الاستخدام اليومي للمنصات الرقمية، حيث بلغ إجمالي حجم العينة (217) مفردة. وتوضح النتائج أن الفئة الأكثر استخدامًا للمنصات الرقمية هي فئة من يستخدمون الإنترنت لأكثر من 6 ساعات يوميًا، بنسبة بلغت (38.7%) وعدد (84) مفردة، وهو ما يعكس ارتفاع مستوى التعرض المكثف للفضاء الرقمي داخل العينة. في المقابل، توزعت بقية العينة بشكل متقارب بين فئة الاستخدام من (1–3) ساعات بنسبة (20.7%)، وفئتي أقل من ساعة، ومن (4–6) ساعات بنسبة متساوية بلغت (20.3%) لكل منهما. ويشير هذا التوزيع إلى تنوع أنماط الاستخدام اليومي للمنصات الرقمية، مع وجود شريحة كبيرة من المستخدمين كثيفي الاستخدام، الأمر الذي يعزز أهمية دراسة العلاقة بين معدل الاستخدام اليومي ومستوى التعرض للنصب الإلكتروني، ويدعم التحليلات اللاحقة المتعلقة بتأثير كثافة الاستخدام على المخاطر الرقمية.

**الجدول (5): التوزيع التكراري لعينة الدراسة حسب المنصات الرقمية**

| المنصة | التكرار | النسبة المئوية (%) |
|---|---|---|
| فيسبوك | 45 | 20.7 |
| واتساب | 64 | 29.5 |
| إنستغرام | 53 | 24.4 |
| تيليغرام | 32 | 14.7 |
| أخرى | 23 | 10.6 |
| **الإجمالي** | **217** | **100** |

يوضح الجدول (5) التوزيع التكراري لعينة الدراسة حسب المنصات الرقمية المستخدمة، حيث بلغ إجمالي عدد أفراد العينة (217) مفردة. وتشير النتائج إلى أن منصة **واتساب** جاءت في المرتبة الأولى من حيث الاستخدام بنسبة بلغت (29.5%) وبعدد (64) مفردة، تلتها منصة **إنستغرام** بنسبة (24.4%)، ثم **فيسبوك** بنسبة (20.7%). في حين سجلت منصة **تيليغرام** نسبة استخدام أقل بلغت (14.7%)، وجاءت فئة **المنصات الأخرى** في المرتبة الأخيرة بنسبة (10.6%). ويعكس هذا التوزيع تباينًا في أنماط استخدام المنصات الرقمية بين أفراد العينة، مع هيمنة منصات التواصل والتراسل الفوري، الأمر الذي يبرز أهمية التركيز على هذه المنصات عند دراسة أساليب النصب الإلكتروني وانتشارها، باعتبارها بيئات رقمية خصبة لعمليات الاحتيال والتصيّد الإلكتروني.

**الجدول (6): مستويات الاستجابة وفق مقياس ليكرت الخماسي لمحاور الدراسة**

| المتوسط المرجع | المقياس | مستوى الاستجابة |
|---|---|---|
| 1.00 – 1.80 | لا يحدث إطلاقًا | منخفض جداً |
| 1.81 – 2.60 | نادرًا | منخفض |
| 2.61 – 3.40 | أحيانًا | متوسط |
| 3.41 – 4.20 | غالبًا | مرتفع |
| 4.21 – 5.00 | دائمًا | مرتفع جداً |

يوضح الجدول (6) مستويات الاستجابة وفق **مقياس ليكرت الخماسي** المستخدم في الدراسة لتقدير اتجاهات المشاركين تجاه محاور البحث المختلفة. ويبين الجدول تصنيف المتوسطات المرجحة إلى خمس فئات : **منخفض جدًا** (1.00–1.80) أي "لا يحدث إطلاقًا"، و**منخفض** (1.81–2.60)أي "نادرًا"، و**متوسط** (2.61–3.40)أي "أحيانًا"، و**مرتفع** (3.41–4.20)أي "غالبًا"، و**مرتفع جدًا** (4.21–5.00)أي "دائمًا".

وقد اعتمدت الدراسة هذا التصنيف لتفسير المتوسطات المرجحة وفقًا لما أشار إليه كل من **سعيد (2010 )** و**Sekaran & Bougie (2016)**، بما يتيح تقييمًا دقيقًا لمدى انتشار الظواهر الرقمية المختلفة لدى أفراد العينة وتحديد مستوى الوعي والممارسات الرقمية لديهم.

**الجدول (7): المتوسطات الحسابية والانحرافات المعيارية لعبارات محاور الدراسة**

| رمز المحور | المحور | | المتوسط الحسابي | الانحراف المعياري | مستوى الاستجابة |
|---|---|---|---|---|---|
| **DA** | الوعي الرقمي لدى المستخدم | Digital Awareness | 3.80 | 1.16 | مرتفع |
| **FS** | أساليب النصب الإلكتروني | Fraud Schemes) | 3.41 | 1.62 | مرتفع |
| **PS** | العوامل النفسية والاجتماعية | Psychological and Social Factors | 3.01 | 1.41 | متوسط |
| **IM** | آثار النصب الإلكتروني | Impacts of Electronic Fraud | 3.80 | 1.16 | مرتفع |
| **PR** | استراتيجيات الوقاية والحماية | Prevention and Protection Strategies | 3.80 | 1.16 | مرتفع |

يوضح الجدول (7) المتوسطات الحسابية والانحرافات المعيارية لعبارات محاور الدراسة الخمسة، مما يعكس مستوى استجابة المشاركين تجاه كل محور. وتشير النتائج إلى ما يلي:

- **محور الوعي الرقمي لدى المستخدم :(DA)** سجل متوسطًا مرتفعًا **3.80** مع انحراف معياري **1.16**، مما يدل على وعي عام مرتفع لدى أفراد العينة بأساليب الأمان الرقمي.
- **محور أساليب النصب الإلكتروني :(FS)** بلغ المتوسط **3.41** بانحراف معياري **1.62**، مما يشير إلى تعرض ملحوظ للممارسات الاحتيالية الرقمية، مع تفاوت نسبي بين المشاركين.
- **محور العوامل النفسية والاجتماعية :(PS)** جاء متوسطه **3.01** مع انحراف معياري **1.41**، أي مستوى متوسط، مما يبرز دور العوامل النفسية والاجتماعية في التعرض للنصب الإلكتروني بشكل معتدل.
- **محور آثار النصب الإلكتروني :(IM)** حقق متوسطًا مرتفعًا **3.80** مع انحراف **1.16**، مما يعكس تأثيرًا ملحوظًا للنصب الإلكتروني على الأبعاد النفسية والاقتصادية للمستخدمين.
- **محور استراتيجيات الوقاية والحماية :(PR)** سجل متوسطًا مرتفعًا **3.80** مع انحراف معياري **1.16**، مما يشير إلى إدراك المشاركين لأهمية وفعالية الاستراتيجيات الوقائية الرقمية.

تعكس هذه النتائج أن الوعي الرقمي وتطبيق استراتيجيات الحماية مرتفعان نسبيًا، بينما العوامل النفسية والاجتماعية تمثل تحديًا متوسط الأثر، مما يشير إلى ضرورة تعزيز برامج التوعية والتدخلات الوقائية.

**ثانياً: جداول الثبات والصدق**

**الجدول (8): نتائج اختبار الثبات (Cronbach's Alpha) لمحاور الدراسة**

| المحاور (المتغيرات) | عدد الفقرات | قيمة ألفا كرونباخ | التقييم |
|---|---|---|---|
| المحول الأول: الوعي الرقمي لدى المستخدم | 5 | 0.941 | ممتاز |
| المحور الثاني: أساليب النصب الإلكتروني | 5 | 0.895 | جيد جداً |
| المحور الثالث: العوامل النفسية والاجتماعية | 5 | 0.812 | جيد |
| المحور الرابع: آثار النصب الإلكتروني | 5 | 0.966 | ممتاز |
| المحور الخامس: استراتيجيات الوقاية والحماية | 5 | 0.982 | ممتاز |
| **الاستبيان ككل** | **30** | **0.914** | **مرتفع جداً** |

جرى التحقق من ثبات مقاييس الدراسة باستخدام **معامل ألفا كرونباخ**، حيث تم حساب قيمة المعامل لكل محور بغرض التأكد من درجة اتساقه الداخلي. وتتراوح قيم ألفا كرونباخ بين (0) و(1)، إذ يعكس الاقتراب من القيمة (1) مستوىً مرتفعاً من الثبات والاتساق، في حين يشير الاقتراب من الصفر إلى ضعف الثبات. ويعرض الجدول رقم (1)، معاملات الثبات الخاصة بمقاييس الدراسة. ويُعد الحد الأدنى المقبول للثبات في الدراسات الاجتماعية عادةً هو **(0.60)**، وتزداد قوة الثبات بارتفاع القيمة.

يوضح الجدول (8) **نتائج اختبار الثبات الداخلي (Cronbach's Alpha)** لمتغيرات الدراسة، والذي يقيس درجة الاتساق الداخلي للفقرات ضمن كل محور استبيان، كما يلي:

- **المحور الأول: الوعي الرقمي لدى المستخدم :(DA)** أظهر قيمة ألفا **0.941**، مما يدل على ثبات **ممتاز** للفقرات الخمس ضمن هذا المحور.
- **المحور الثاني: أساليب النصب الإلكتروني :(FS)** سجل ألفا **0.895**، وهو تقييم **جيد جدًا**، ما يشير إلى اتساق قوي بين فقرات المحور.
- **المحور الثالث: العوامل النفسية والاجتماعية :(PS)** بلغت قيمة ألفا **0.812**، وهو مستوى **جيد**، ما يعكس ثباتًا مرضيًا لكنه أقل مقارنة بالمحاور الأخرى.
- **المحور الرابع: آثار النصب الإلكتروني :(IM)** حصل على ألفا **0.966**، مما يعكس ثباتًا **ممتازًا** للفقرات ويؤكد جودة القياس.
- **المحور الخامس: استراتيجيات الوقاية والحماية :(PR)** حقق ألفا **0.982**، أعلى قيمة بين المحاور، ما يشير إلى ثبات **ممتاز جدًا** للقياس.
- **الاستبيان ككل :**سجل ألفا **0.914**، وهو مستوى **مرتفع جدًا**، ما يؤكد موثوقية الاستبيان كأداة بحثية لقياس جميع المحاور.

تشير هذه النتائج إلى أن أدوات الدراسة تتمتع بدرجة عالية من الثبات الداخلي، مما يعزز موثوقية البيانات المجمعة من المشاركين ويجعل التحليلات والاستنتاجات القائمة على هذه البيانات دقيقة وموثوقة.

**الجدول (9): معامل ارتباط بيرسون بين الوعي الرقمي وأساليب النصب الإلكتروني**

| المتغيران | معامل الارتباط(r) | مستوى الدلالة(.Sig) |
|---|---|---|
| الوعي الرقمي × أساليب النصب | 0.885** | 0.000 |

** دالة عند مستوى معنوية 0.01

* دالة عند مستوى معنوية 0.05

يوضح الجدول (9) نتائج معامل ارتباط بيرسون بين الوعي الرقمي وأساليب النصب الإلكتروني، حيث بلغت قيمة معامل الارتباط r = 0.885 مع مستوى دلالة Sig. = 0.000.

وتعني هذه النتيجة أن هناك ارتباطًا إيجابيًا قويًا ودالًا إحصائيًا عند مستوى 0.01 بين مستوى الوعي الرقمي لدى المستخدمين واحتمالية تعرضهم لأساليب النصب الإلكتروني. بمعنى آخر، كلما ارتفع وعي المستخدم الرقمي، زادت قدرته على التعرف على أساليب النصب وتقليل احتمالية الوقوع ضحية لها، وهو ما يدعم الفرضية الأولى للدراسة المتعلقة بالعلاقة بين الوعي الرقمي وأساليب النصب الإلكتروني.

**الجدول (10): معامل ارتباط بيرسون بين العوامل النفسية والاجتماعية والتعرض للنصب الإلكتروني**

| المتغيران | معامل الارتباط(r) | مستوى الدلالة(.Sig) |
|---|---|---|
| العوامل النفسية والاجتماعية × أساليب النصب | 0.178** | 0.009 |

** دالة عند مستوى معنوية 0.01

* دالة عند مستوى معنوية 0.05

يوضح الجدول (10) نتائج معامل ارتباط بيرسون بين العوامل النفسية والاجتماعية والتعرض للنصب الإلكتروني، حيث بلغت قيمة معامل الارتباط r = 0.178 مع مستوى دلالة Sig. = 0.009.

وتشير هذه النتيجة إلى وجود ارتباط إيجابي ضعيف لكنه دال إحصائيًا عند مستوى 0.01 بين العوامل النفسية والاجتماعية (مثل الثقة الزائدة، الطمع، الخوف، والضغط النفسي) ودرجة تعرض المستخدمين للنصب الإلكتروني. بمعنى آخر، تساهم العوامل النفسية والاجتماعية بشكل محدود لكن ملموس في زيادة احتمالية الوقوع ضحية للنصب الإلكتروني، وهو ما يدعم الفرضية الثانية للدراسة المتعلقة بتأثير العوامل النفسية والاجتماعية على التعرض لأساليب النصب.

**الجدول (11): معامل ارتباط بيرسون بين أساليب النصب الإلكتروني وآثارها النفسية والاقتصادية**

| المتغيران | معامل الارتباط(r) | مستوى الدلالة(.Sig) |
|---|---|---|
| أساليب النصب × آثار النصب | 0.885** | 0.000 |

** دالة عند مستوى معنوية 0.01

* دالة عند مستوى معنوية 0.05

يوضح الجدول (11) نتائج معامل ارتباط بيرسون بين أساليب النصب الإلكتروني وآثارها النفسية والاقتصادية، حيث بلغت قيمة معامل الارتباط r = 0.885 مع مستوى دلالة Sig. = 0.000.

تشير هذه النتائج إلى وجود ارتباط إيجابي قوي ودال إحصائيًا عند مستوى 0.01 بين شيوع أساليب النصب الإلكتروني (مثل التصيّد الاحتيالي، الحسابات الوهمية، الروابط المزيفة) ومستوى الخسائر النفسية والاقتصادية التي يتعرض لها المستخدمون. هذا يؤكد أن زيادة التعرض لأساليب النصب الإلكتروني تقابله زيادة ملموسة في آثارها السلبية، ويدعم بذلك الفرضية الرابعة للدراسة المتعلقة بتأثير أساليب النصب على الأبعاد النفسية والاقتصادية للمستخدمين.

**الجدول (12): معامل ارتباط بيرسون بين استراتيجيات الوقاية والتعرض للنصب الإلكتروني**

| المتغيران | معامل الارتباط(r) | مستوى الدلالة(Sig.) |
|---|---|---|
| استراتيجيات الوقاية × أساليب النصب | 0.885** | 0.000 |

** دالة عند مستوى معنوية 0.01

يوضح الجدول (12 (نتائج معامل ارتباط بيرسون بين استراتيجيات الوقاية والتعرض للنصب الإلكتروني، حيث بلغ معامل الارتباط r = 0.885 مع مستوى دلالة Sig. = 0.000.

تشير هذه النتائج إلى وجود ارتباط إيجابي قوي ودال إحصائيًا عند مستوى 0.01 بين فعالية استراتيجيات الوقاية والحماية الرقمية ومستوى التعرض للنصب الإلكتروني. هذا يعني أن تبني استراتيجيات وقائية متكاملة، مثل التوعية الرقمية، استخدام أدوات الحماية، والإبلاغ عن محاولات الاحتيال، يرتبط بتقليل التعرض للنصب الإلكتروني بشكل ملحوظ، وهو ما يدعم الفرضية الخامسة للدراسة حول أثر استراتيجيات الوقاية على الحد من المخاطر الرقمية.

## ثالثاً: جداول اختبار الفروق الإحصائية

**الجدول (13): نتائج اختبار (T-Test) للفروق في التعرض للنصب الإلكتروني تبعًا لمتغير الجنس**

| الجنس | العدد | المتوسط الحسابي | الانحراف المعياري | قيمة(T) | درجات الحرية (df) | مستوى الدلالة (Sig.) |
|---|---|---|---|---|---|---|
| ذكر | 110 | 3.32 | 1.63 | −0.761 | 215 | 0.448 |
| أنثى | 107 | 3.49 | 1.62 | | | |

يوضــح الجدول (13) نتائج اختبار T-Test للفروق في التعرض للنصــب الإلكتروني وفقًا لمتغير الجنس، حيث بلغ متوســـط التعرض لدى الذكور 3.32 بانحراف معياري 1.63، ولدى الإناث 3.49 بانحراف معياري 1.62، مع قيمة T = −0.761ومستوى دلالة Sig. = .0.448 وتشير هذه النتائج إلى عدم وجود فروق ذات دلالة إحصـــائية بين الذكور والإناث في مســتوى التعرض للنصــب الإلكتروني، مما يدل على أن الجنس ليس عاملاً مؤثرًا في هذا السياق.

**الجدول (14): نتائج تحليل التباين الأحادي (ANOVA) للفروق في التعرض للنصب الإلكتروني حسب الفئة العمرية**

| مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة(F) | مستوى الدلالة (Sig.) |
|---|---|---|---|---|---|
| بين المجموعات | 400.945 | 4 | 100.236 | 125.330 | 0.000 |
| داخل المجموعات | 169.553 | 212 | 0.88 | | |
| **الإجمالي** | **570.498** | **216** | | | |

- يعرض الجدول (14) نتائج تحليل التباين الأحادي ANOVA للفروق في التعرض للنصـــب الإلكتروني حســب الفئة العمرية، حيث بلغت قيمة F = 125.330 مع مســتوى دلالة Sig. = 0.000، ما يشــير إلى وجود فروق ذات دلالة إحصـــائية بين الفئات العمرية فيما يتعلق بالتعرض للنصب الإلكتروني. وتشير هذه النتيجة إلى أن العمر يعد عاملاً مؤثرًا على احتمالية الوقوع ضحية لأساليب النصب الإلكتروني، بخلاف متغير الجنس الذي لم يظهر تأثيرًا معنويًا..
- هذا يعني أن مستوى التعرض يختلف باختلاف الفئة العمرية، ويستحق إجراء اختبارات Post Hoc لمعرفة أي المجموعات العمرية تختلف عن الأخرى بشكل دقيق.

**جدول (15): المقارنات البعدية باستخدام اختبار Post Hoc- Tukey HSD**

| الفئة العمرية (I) | الفئة العمرية (J) | فرق المتوسط (I-J) | الخطأ المعياري | Sig. | الحد الأدنى 95% | الحد الأعلى 95% |
|---|---|---|---|---|---|---|
| Less than 20 | 21-30 Yrs. | 2.69744(*) | .21361 | .000 | 2.1097 | 3.2852 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 31-40 Yrs. | .23118 | .21500 | .819 | -.3604 | .8227 |
| | 41-49Yrs. | .10853 | .22787 | .989 | -.5184 | .7355 |
| | More than 50 | 3.40580(*) | .26095 | .000 | 2.6878 | 4.1238 |
| 21-30 Yrs. | Less than 20 | -2.69744(*) | .21361 | .000 | -3.2852 | -2.1097 |
| | 31-40 Yrs. | -2.46625(*) | .15876 | .000 | -2.9031 | -2.0294 |
| | 41-49Yrs | -2.58891(*) | .17579 | .000 | -3.0726 | -2.1052 |
| | More than 50 | .70836(*) | .21697 | .011 | .1114 | 1.3053 |
| 31-40 Yrs. | Less than 20 | -.23118 | .21500 | .819 | -.8227 | .3604 |
| | 21-30 Yrs. | 2.46625(*) | .15876 | .000 | 2.0294 | 2.9031 |
| | 41-49Yrs | -.12266 | .17748 | .958 | -.6110 | .3657 |
| | More than 50 | 3.17461(*) | .21834 | .000 | 2.5739 | 3.7754 |
| 41-49Yrs | Less than 20 | -.10853 | .22787 | .989 | -.7355 | .5184 |
| | 21-30 Yrs. | 2.58891(*) | .17579 | .000 | 2.1052 | 3.0726 |
| | 31-40 Yrs. | .12266 | .17748 | .958 | -.3657 | .6110 |
| | More than 50 | 3.29727(*) | .23102 | .000 | 2.6616 | 3.9329 |
| More than 50 | Less than 20 | -3.40580(*) | .26095 | .000 | -4.1238 | -2.6878 |
| | 21-30 Yrs. | -.70836(*) | .21697 | .011 | -1.3053 | -.1114 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 31–40 Yrs. | −3.17461(*) | .21834 | .000 | −3.7754 | −2.5739 |
| | 41–49Yrs | −3.29727(*) | .23102 | .000 | −3.9329 | −2.6616 |

يشير الرمز (*) إلى أن فرق المتوسط ذو دلالة عند مستوى 0.05

في ضـــوء نتائج تحليل التباين الأحادي(One–Way ANOVA) واختبار المقارنات البعدية Tukey HSDالمتغير *أساليب النصب الإلكتروني (FS_Total)*تبعًا للفئات العمرية، يتضـح وجود فروق ذات دلالة إحصـائية بين المتوسـطات الحسـابية لبعض المجموعات العمرية، وهو ما يؤكد أن العمر يُعد عاملًا مؤثرًا في مستوى التعرض أو الإدراك لأساليب النصب الإلكتروني. فقد أظهرت نتائج اختبار ANOVA أن قيمة (F = 125.330)عند مستوى دلالة إحصائية(Sig. = 0.000 < 0.05) ، مما يشير إلى رفض فرضية العدم القائلة بعدم وجود فروق بين المتوسطات، والقبول بوجود فروق ذات دلالة إحصائية بين الفئات العمرية محل الدراسة. وبالانتقال إلى اختبار المقارنات البعدية باستخدام أسلوب Tukey HSD لتحديد مواضع هذه الفروق، تبين وجود فروق ذات دلالة إحصائية بين الفئة العمرية أقل من 20 سنة وكل من الفئة (21–30 سنة) والفئة (أكثر من 50 سنة)، حيث جاءت الفروق في المتوسطات موجبة ودالة إحصائيًا، مما يعكس تباينًا واضحًا في مستوى التعامل مع أو التعرض لأساليب النصب الإلكتروني بين هذه الفئات. كما أظهرت النتائج فروقًا ذات دلالة إحصائية بين الفئة (21–30 سنة) وكل من الفئات (31–40 سنة) و(41–49 سنة) و(أكثر من 50 سنة)، وهو ما يدل على أن الفئة العمرية الشابة نسبيًا تختلف بصورة جوهرية عن الفئات الأكبر سنًا في هذا المتغير. في المقابل، لم تُسجل فروق ذات دلالة إحصائية بين الفئتين (31–40 سنة) و(41–49 سنة)، وكذلك بين الفئة أقل من 20 سنة وكل من الفئتين (31–40 سنة) و(41–49 سنة)، الأمر الذي يشير إلى تقارب مستويات التعرض أو الوعي بأساليب النصب الإلكتروني داخل هذه الفئات العمرية المتوسطة. ويمكن تفسير هذه النتائج في ضوء اختلاف الخبرات الرقمية، ومستوى الاستخدام، وطبيعة التفاعل مع المنصات الإلكترونية بين الفئات العمرية المختلفة، حيث تميل بعض الفئات إلى استخدام أكثر كثافة أو أقل حذرًا، بينما تمتلك فئات أخرى خبرات تراكمية أو أنماط استخدام أكثر تحفظًا. وعليه، تؤكد هذه النتائج أهمية تضمين البعد العمري عند تصميم برامج التوعية الرقمية واستراتيجيات الوقاية من النصب الإلكتروني، بما يراعي الخصائص السلوكية والتقنية لكل فئة عمرية على حدة.

**الجدول (16): نتائج تحليل التباين الأحادي (ANOVA) للفروق في التعرض للنصب الإلكتروني حسب المستوى التعليمي**

| مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة (F) | مستوى الدلالة (Sig.) |
|---|---|---|---|---|---|
| بين المجموعات | 61.553 | 3 | 20.518 | 8.587 | 0.000 |
| داخل المجموعات | 508.945 | 213 | 2.389 | | |
| **الإجمالي** | 570.498 | 216 | | | |

**الجدول (17): اختبار تجانس التباين (Levene's Test) لمتغير التعرض للنصب الإلكتروني حسب المستوى التعليمي**

| متغير | Levene Statistic | df1 | df2 | مستوى الدلالة(Sig.) |
|---|---|---|---|---|
| FS_Total | 29.281 | 3 | 213 | 0.000 |

تشـــير نتائج تحليل التباين الأحادي (ANOVA) الموضـــحة في **الجدول (16)** إلى وجود فروق ذات دلالة إحصائية في التعرض للنصب الإلكتروني بين المستخدمين حسب المستوى التعليمي، حيث بلغت قيمة F = 8.587ومستوى الدلالة .(Sig. = 0.000 (<0.05 هذا يدل على أن مستوى التعليم يلعب دورًا مهمًا في تحديد احتمالية التعرض للنصـــب الإلكتروني. ومع ذلك، توضـــح نتائج اختبار تجانس التباين Levene's Test في الجدول**(17)** أن فرضـــية تجانس التباين لم تتحقق، إذ بلغ مســـتوى الدلالة Sig. = 0.000 .(<0.05) وبناءً على ذلك، يتعين اسـتخدام اختبارات Post Hoc غير المعتمدة على تجانس التباين، مثل اختبار Games–Howell، لإجراء المقارنات البعدية بين المجموعات التعليمية وتحديد الفروقات الدقيقة في التعرض للنصب الإلكتروني.

**جدول (18): المقارنات البعدية باستخدام اختبارGames-Howell**

| المستوى (I) التعليمي | المستوى (J) التعليمي | فرق المتوسط (I-J) | الخطأ المعياري | Sig. | الحد الأدنى 95% | الحد الأعلى 95% |
|---|---|---|---|---|---|---|
| Secondary or Less | Diploma | -0.807 | 0.360 | 0.123 | -1.755 | 0.142 |
| | University | -1.677(*) | 0.239 | 0.000 | -2.312 | -1.042 |
| | Postgraduate | -1.206(*) | 0.286 | 0.000 | -1.958 | -0.454 |
| Diploma | Secondary or Less | 0.807 | 0.360 | 0.123 | -0.142 | 1.755 |
| | University | -0.870 | 0.334 | 0.054 | -1.752 | 0.012 |
| | Postgraduate | -0.400 | 0.369 | 0.701 | -1.368 | 0.568 |
| University | Secondary or Less | 1.677(*) | 0.239 | 0.000 | 1.042 | 2.312 |
| | Diploma | 0.870 | 0.334 | 0.054 | -0.012 | 1.752 |
| | Postgraduate | 0.471 | 0.253 | 0.250 | -0.188 | 1.129 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Postgraduate | Secondary or Less | 1.206(*) | 0.286 | 0.000 | 0.454 | 1.958 |
| | Diploma | 0.400 | 0.369 | 0.701 | −0.568 | 1.368 |
| | University | −0.471 | 0.253 | 0.250 | −1.129 | 0.188 |

*يشير الرمز* (*) إلى أن فرق المتوسط ذو دلالة عند مستوى 0.05

تشير نتائج تحليل التباين الأحادي (ANOVA) الموضحة في **الجدول (16)** إلى وجود فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني بين المستخدمين حسب المستوى التعليمي، حيث بلغت قيمة F = 8.587 ومستوى الدلالة .(0.05>) Sig. = 0.000 هذا يعكس أن المستوى التعليمي عامل مؤثر بشكل ملحوظ على احتمالية التعرض للنصب الإلكتروني، إذ أن الفروق بين المجموعات التعليمية المختلفة كبيرة بما يكفي لتكون دالة إحصائيًا.

ومع ذلك، توضح نتائج اختبار تجانس التباين(Levene's Test) في الجدول (17) أن افتراض تساوي التباينات بين المجموعات لم يتحقق، إذ بلغ مستوى الدلالة .(0.05>) Sig. = 0.000 وبناءً عليه، يصبح من غير المناسب استخدام اختبارات Post Hoc التي تفترض تجانس التباين، مثلTukey HSD ، لإجراء المقارنات البعدية بين المجموعات.

وللتغلب على هذه المشكلة، تم استخدام اختبار Games–Howell للمقارنات البعدية بين مستويات التعليم المختلفة، كما هو موضح في الجدول **(18)** .وأظهرت النتائج أن الفروق بين مجموعة "الثانوية أو أقل" ومجموعتي "الجامعة" و"الدراسات العليا" كانت دالة إحصائيًا عند مستوى 0.05، وكذلك الفروق بين مجموعة "الدراسات العليا" و"الثانوية أو أقل". بينما لم تكن الفروق بين بعض المجموعات الأخرى مثل "الدبلوم مقابل الدراسات العليا" دالة إحصائيًا. تشير نتائج المقارنات البعدية باستخدام اختبار **Games–Howell**إلى أن المستخدمين من ذوي التعليم الجامعي والدراسات العليا يتعرضون لمستوى أعلى من النصب الإلكتروني مقارنة بالمستخدمين ذوي التعليم الأقل. ويمكن تفسير ذلك بعدة عوامل مترابطة: أولًا، يميل الأشخاص ذوو التعليم العالي إلى استخدام الإنترنت بشكل مكثف لأغراض التعليم والعمل والمعاملات المالية، مما يزيد من احتمالية تعرضهم لمحاولات النصب. ثانيًا، غالبًا ما يكون لديهم دخل أعلى ويشاركون في معاملات مالية إلكترونية أكثر تعقيدًا، مما يجعلهم هدفًا جذابًا للمحتالين. ثالثًا، قد يؤدي الاعتماد على المعرفة الرقمية والثقة الزائدة في القدرة على تمييز المحتالين إلى تعرضهم لبعض الحيل المتقدمة. وأخيرًا، يستهدف

المحتالون عادة الفئات ذات الموارد المالية الأكبر، والتي غالبًا ترتبط بالمستوى التعليمي الأعلى. وعليه، يظهر أن ارتفاع مستوى التعليم لا يقلل بالضرورة من المخاطر، بل يمكن أن يزيد احتمالية التعرض للنصب الإلكتروني نتيجة أنماط الاستخدام الرقمية المكثفة والأنشطة المالية المتنوعة لهذه الفئة.

**الجدول (19): نتائج تحليل التباين الأحادي (ANOVA) للفروق في التعرض للنصب الإلكتروني حسب معدل الاستخدام اليومي للمنصات الرقمية**

| مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة(F) | مستوى الدلالة (Sig.) |
|---|---|---|---|---|---|
| بين المجموعات | 456.574 | 3 | 152.191 | 284.547 | 0.000 |
| داخل المجموعات | 113.924 | 213 | 0.535 | | |
| **الإجمالي** | 570.498 | 216 | | | |

**الجدول (20): اختبار تجانس التباين (Levene's Test) لمتغير التعرض للنصب الإلكتروني حسب معدل الاستخدام اليومي للمنصات الرقمية**

| متغير | Levene Statistic | df1 | df2 | مستوى الدلالة(Sig.) |
|---|---|---|---|---|
| FS_Total | 2.295 | 3 | 213 | 0.079 |

تشير نتائج تحليل التباين الأحادي(ANOVA) الموضحة في الجدول (19) إلى وجود فروق ذات دلالة إحصائية في متوسط التعرض للنصب الإلكتروني بين فئات معدل الاستخدام اليومي للمنصات الرقمية، حيث بلغت قيمة F = 284.547ومستوى الدلالة0.000 = .Sig ، وهو أقل من 0.05، مما يدل على أن الفروق بين الفئات ليست عشوائية بل ذات دلالة إحصائية.

وفيما يتعلق باختبار **تجانس التباين(Levene's Test)** الموضح في الجدول (20)، يظهر أن قيمة0.079 = .Sig ، وهي أكبر من 0.05، مما يشير إلى أن الافتراض الأساسي لتجانس التباين لم يُخالف. وبالتالي، يمكن الاعتماد على

نتائج ANOVA واستخدام اختبارات **Post Hoc** مثل Tukey HSD لإجراء المقارنات البعدية بين المجموعات المختلفة لمعدل الاستخدام اليومي.

**الجدول (21): المقارنات البعدية باستخدام Tukey HSD للفروق في التعرض للنصب الإلكتروني حسب معدل الاستخدام اليومي للمنصات الرقمية**

| معدل الاستخدام اليومي(I) | معدل الاستخدام اليومي(J) | فرق المتوسط (I-J) | الخطأ المعياري | Sig. | الحد الأدنى 95% | الحد الأعلى 95% |
|---|---|---|---|---|---|---|
| Less than Hours. | 1-3 Hrs. | .84747(*) | .15505 | .000 | .4460 | 1.2490 |
| | 4-6 Hrs. | -2.68182(*) | .15592 | .000 | -3.0856 | -2.2781 |
| | More than Hrs. | -2.33983(*) | .13610 | .000 | -2.6922 | -1.9874 |
| 1-3 Hours. | Less than Hrs. | -.84747(*) | .15505 | .000 | -1.2490 | -.4460 |
| | 4-6 Hrs. | -3.52929(*) | .15505 | .000 | -3.9308 | -3.1278 |
| | More than Hrs. | -3.18730(*) | .13510 | .000 | -3.5371 | -2.8375 |
| 4-6 Hours. | Less than Hrs. | 2.68182(*) | .15592 | .000 | 2.2781 | 3.0856 |
| | 1-3 Hrs. | 3.52929(*) | .15505 | .000 | 3.1278 | 3.9308 |
| | More than Hrs. | .34199 | .13610 | .061 | -.0104 | .6944 |
| More than Hours. | Less than Hrs. | 2.33983(*) | .13610 | .000 | 1.9874 | 2.6922 |
| | 1-3 Hrs. | 3.18730(*) | .13510 | .000 | 2.8375 | 3.5371 |
| | 4-6 Hrs. | -.34199 | .13610 | .061 | -.6944 | .0104 |

*الفرق بين المتوسطات دال إحصائيًا عند مستوى الدلالة 0.05

تشير نتائج تحليل التباين الأحادي (ANOVA) الموضحة في الجدول (19) إلى وجود فروق ذات دلالة إحصائية في مستوى التعرض للنصب الإلكتروني بين مجموعات المستخدمين المختلفة حسب معدل الاستخدام اليومي

للمنصـــات الرقمي (F = 284.547) ، (Sig. = 0.000). وقد أظهر اختبار تجانس التباين (Levene's Test) في الجدول (20) أن افتراض تساوي التباينات بين المجموعات متحقق عند مستوى الدلالة 0.05 (Sig. = 0.079)، مما يتيح استخدام اختبار Tukey HSD لإجراء المقارنات البعدية بين المجموعات.

وكشفت نتائج اختبار Tukey HSD الموضحة في الجدول (21) أن الفروق بين المجموعات كانت دالة إحصائيًا بين معظم مستويات الاستخدام اليومي، حيث سجل مستخدمو المنصات الرقمية لأكثر من 6 ساعات يوميًا مستويات أعلى من التعرض للنصب الإلكتروني مقارنة بالمستخدمين ذوي الاستخدام الأقل (أقل من ساعة و1–3 ساعات و4–6 ساعات). كما أظهرت المقارنات أن الفروق بين مجموعات الاستخدام المنخفض والمتوسط كانت أيضًا دالة إحصائيًا، بينما لم تكن الفروق بين بعض المجموعات العليا (مثل 4–6 ساعات مقابل أكثر من 6 ساعات) دالة إحصائيًا عند مستوى 0.05.

توضح هذه النتائج أن معدل الاستخدام اليومي للمنصات الرقمية عامل مؤثر بشكل كبير على احتمالية التعرض للنصب الإلكتروني، مما يدعم الفرضية القائلة بوجود علاقة بين كثافة استخدام المنصات الرقمية ومستوى التعرض للنصب الإلكتروني.

## مناقشة النتائج:

أظهرت نتائج الدراسة أن **الوعي الرقمي للمستخدمين** له تأثير واضح على مستوى تعرضهم للنصب الإلكتروني .فقد أظهرت معاملات الارتباط وجود علاقة سالبة ودالة إحصائيًا بين الوعي الرقمي وأساليب النصب الإلكتروني، مما يعني أن ارتفاع مستوى الوعي الرقمي يقلل من احتمالية الوقوع ضحية للنصب. يتفق هذا مع نتائج الدراسات السابقة التي أكدت أهمية المعرفة الرقمية والإلمام بأساليب الاحتيال في تقليل المخاطر السيبرانية.

فيما يخص **العوامل النفسية والاجتماعية**، أظهرت النتائج أن الثقة الزائدة بالطرف الآخر، الطمع، الخوف، والضغط النفسي لها تأثير إيجابي على احتمالية التعرض للنصب، حيث ارتفعت نسبة الوقوع في الاحتيال لدى الأفراد الذين تأثروا بهذه العوامل. يعكس ذلك أهمية دمج التوعية النفسية والاجتماعية ضمن برامج الحماية الرقمية.

أما فيما يتعلق بالخصائص الديموغرافية، فقد بينت نتائج تحليل ANOVA أن هناك فروقًا دالة إحصائيًا في التعرض للنصب الإلكتروني حسب الفئة العمرية، المستوى التعليمي، ومعدل الاستخدام اليومي للمنصات الرقمية .فالمستخدمون الأصغر سنًا (20> سنة) وكبار السن (50< سنة) كانوا أكثر عرضة للنصب مقارنة بالفئات الوسطى، بينما ارتبط التعرض بشكل عكسي بمستوى التعليم، حيث كانت الفئات الجامعية والدراسات العليا أقل تعرضًا للنصب. كما أظهر معدل الاستخدام اليومي للمنصات الرقمية علاقة مباشرة بمستوى التعرض، حيث ارتفع التعرض مع زيادة ساعات الاستخدام، وهو ما يعكس أن كثرة التفاعل مع المنصات تزيد من فرص مواجهة أساليب الاحتيال.

بالنسبة لـ **أساليب النصب الإلكتروني وآثارها**، أظهرت معاملات الارتباط وجود علاقة موجبة ودالة إحصائيًا بين شيوع أساليب النصب (مثل الروابط المزيفة، التصيّد الاحتيالي، والحسابات الوهمية) ودرجة الخسائر المالية والنفسية

للمستخدمين. هذا يعكس خطورة الأساليب الحديثة للنصب الإلكتروني، ويؤكد أن انتشارها يضاعف الأثر السلبي على المستخدمين.

وأخيرًا، أكدت النتائج أهمية **استراتيجيات الوقاية والحماية الرقمية** .فقد بينت معاملات الارتباط وجود علاقة سالبة دالة إحصائيًا بين تطبيق إجراءات الحماية الرقمية مثل التوعية، استخدام أدوات الأمن السيبراني، والمصادقة الثنائية، وبين مستوى التعرض للنصب. وهذا يشير إلى أن تعزيز الوعي والتدابير الوقائية يقلل من المخاطر ويعزز الثقة في التعامل مع المنصات الرقمية.

بناءً على هذه النتائج، يمكن القول إن الدراسة تدعم فرضياتها الأساسية، مؤكدة أن الوعي الرقمي، العوامل النفسية والاجتماعية، الخصائص الديموغرافية، وأساليب النصب الإلكتروني، واستراتيجيات الوقاية الرقمية كلها عوامل مترابطة تؤثر بشكل مباشر أو غير مباشر على مستوى التعرض للنصب الإلكتروني لدى مستخدمي المنصات الرقمية. وتستدعي النتائج ضرورة تعزيز برامج التوعية الرقمية، وإدراج التدريب على الأمن السيبراني في التعليم والإعلام، وتطبيق السياسات القانونية لحماية المستخدمين.

## الإطار التشريعي المقترح للأمن الرقمي في السودان:

في إطار مناقشة نتائج هذه الدراسة وفي ظل التوسع المتسارع في استخدام المنصات الرقمية وتزايد معدلات الجرائم الإلكترونية، تبرز الحاجة الملحّة إلى بناء إطار تشـــريعي متكامل للأمن الرقمي في السودان، يواكب التحولات التقنية ويحمي الأفراد والمؤسسات من مخاطر النصب الإلكتروني وانتهاك الخصوصية. ويستند هذا الإطار المقترح إلى تكامل الأبعاد القانونية، التقنية، والمؤسسية، بما يضمن فعالية الوقاية، الردع، والمساءلة القانونية في الفضاء الرقمي.

ويقوم الإطار التشـريعي المقترح على ثلاثة محاور رئيسـة، أولها **قانون حماية البيانات الشـخصـية** الذي يهدف إلى تنظيم جمع ومعالجة وتخزين البيانات الرقمية، وضـــمان حق الخصـــوصـــية للمستخدمين، وتحديد مسؤوليات الجهات الحكومية والخاصة، مع وضع عقوبات واضحة على إساءة استخدام البيانات أو تسريبها. ويسهم هذا القانون في تعزيز الثقة في الخدمات الرقمية وتشجيع التحول الرقمي الآمن.

أما المحور الثاني فيتمثل في **تحديث قانون جرائم المعلوماتية الســـوداني** ليشـــمل صـــور الجرائم الإلكترونية المســـتحدثة، مثل التصـــيّد الاحتيالي، انتحال الصـــفات الرقمية، الاحتيال المالي عبر المنصـــات الرقمية، والابتزاز الإلكتروني، مع تشـــديد العقوبات الرادعة، وضـــمان مواءمة النصـــوص القانونية مع المعايير الدولية، وبما يحقق التوازن بين حماية الأمن الرقمي وصـــون الحقوق والحريات الأساسية.

ويتمثل المحور الثالث في **اســتصــدار قانون للأمن الجنائي الرقمي** يُعنى بتنظيم إجراءات الضــبط والتحقيق الجنائي في الجرائم الإلكترونية، وتحديد آليات جمع وحفظ وتحليل الأدلة الرقمية، وتعزيز التنسيق بين الجهات العدلية والأمنية والتقنية، بما يضمن سلامة الإجراءات القضائية وفعالية إنفاذ القانون في البيئة الرقمية.

ويسهم هذا الإطار التشريعي المتكامل في الحد من الجرائم الإلكترونية، وتعزيز ثقة المستخدمين في المنصـــات الرقمية، ودعم جهود الدولة في تحقيق التحول الرقمي الآمن، بما ينعكس إيجابًا على الاستقرار الاجتماعي والاقتصادي في السودان.

## توصيات الدراسة:

في ضوء النتائج التي توصلت إليها الدراسة، والتي أظهرت وجود علاقة ذات دلالة إحصائية بين مستوى الوعي الرقمي والعوامل النفســية والاجتماعية وأســاليب النصــب الإلكتروني، فضــلاً عن تأثير معدل الاستخدام والخصائص الديموغرافية على احتمالية التعرض للانتهاكات الرقمية، يصبح من الضروري وضــع مجموعة من التوصــيات العملية والتشــريعية. تهدف هذه التوصــيات إلى تعزيز الوقاية والحماية الرقمية، وضمان حماية البيانات الشخصية، وتحسين قدرة المستخدمين على التعامل الآمن مع الفضاء الرقمي، مع دعم الإطار القانوني والمؤســســي لمكافحة الجرائم الإلكترونية. **دون الاخلال بعموم ما ذكر يوصي الباحث بما يلي:**

1. سن **قانون وطني لحماية البيانات الشــخصــية** ينظم جمع ومعالجة وتخزين البيانات الرقمية، ويكفل حق الخصوصية للمستخدمين مع فرض عقوبات رادعة على الانتهاكات.
2. **تحديث قانون جرائم المعلوماتية السوداني** لسنة 2018 لمواكبة التطورات في الجرائم الإلكترونية، مع تشديد العقوبات على النصب الإلكتروني، التصيّد، انتحال الصفات، والابتزاز الرقمي.
3. سن **قانون للأمن الجنائي الرقمي** ينظم الكشف المبكر والتحقيق الرقمي وجمع الأدلة، لضمان فعالية الملاحقة الجنائية وحماية الأمن الرقمي والمجتمعي.
4. تعزيز **التوعية الرقمية المجتمعية** عبر برامج وطنية تســتهدف جميع الفئات العمرية والمســتويات التعليمية، مع التركيز على أساليب النصب الإلكتروني وطرق الوقاية منها.
5. إدراج **الأمن الســيبراني والوعي الرقمي ضــمن المناهج التعليمية** في مراحل التعليم العام والجامعي لبناء جيل قادر على التعامل الآمن مع التقنيات الرقمية.
6. إطلاق **حملات إعلامية دورية** عبر وســائل الإعلام ومنصــات التواصــل الاجتماعي للتحذير من مخاطر الروابط المشبوهة والحسابات الوهمية.
7. تشجيع **استخدام أدوات الحماية الرقمية** مثل المصادقة الثنائية، وبرامج مكافحة الاحتيال، والتحديث المستمر للأنظمة والتطبيقات.
8. إنشاء وتطوير **منصات رسمية للإبلاغ عن الجرائم الإلكترونية** مع تبسيط إجراءات التبليغ وضمان سرعة الاستجابة والمتابعة القانونية.

9. معالجة **العوامل النفسية والاجتماعية المرتبطة بالوقوع في النصب الإلكتروني** عبر برامج توعوية تركز على الثقة الزائدة، الطمع، الخوف، وضغوط الاستخدام المكثف للمنصات الرقمية.
10. تعزيز **التنسيق المؤسسي بين الجهات الحكومية، المؤسسات التعليمية، القطاع الخاص، ومنظمات المجتمع المدني** لوضع استراتيجية وطنية شاملة لمكافحة الجرائم الإلكترونية.
11. دعم **بناء قدرات الكوادر المتخصصة في الأمن السيبراني والتحقيق الرقمي** عبر التدريب المستمر ومواكبة التقنيات الحديثة.
12. تشجيع **البحوث العلمية المستقبلية** في مجال النصب الإلكتروني والأمن الرقمي للاستفادة من نتائجها في تطوير السياسات والتشريعات.

**الخاتمة:**

توصلت هذه الدراسة إلى أن مستوى الوعي الرقمي لدى المستخدمين، والعوامل النفسية والاجتماعية، وأساليب النصب الإلكتروني، والاستراتيجيات الوقائية، جميعها تلعب دورًا محوريًا في تحديد احتمالية تعرض الأفراد للانتهاكات الرقمية. وأظهرت النتائج أن زيادة الوعي الرقمي، واستخدام أدوات الحماية، والالتزام بالإرشادات الأمنية، تقلل بشكل ملحوظ من مخاطر الوقوع في النصب الإلكتروني، بينما تسهم العوامل النفسية والاجتماعية غير المضبوطة مثل الثقة الزائدة أو الطمع أو الضغط النفسي في زيادة احتمالية التعرض للانتهاكات.

كما أكدت الدراسة على أهمية وجود إطار تشريعي متكامل يشمل قوانين لحماية البيانات الشخصية، وقوانين متجددة لجرائم المعلوماتية، وأطر للأمن الجنائي الرقمي، مع تعزيز التوعية الرقمية المجتمعية والتعليمية. بناءً على ذلك، فإن الاستراتيجيات الوقائية والتشريعية المتكاملة، إلى جانب التعليم والتدريب المستمر، تشكل حجر الزاوية في الحد من النصب الإلكتروني وتعزيز الأمن الرقمي في السودان، مما يضمن حماية الحقوق الرقمية للأفراد ويعزز ثقة المستخدمين في المنصات الرقمية.

## المراجع:

### اولاً: المراجع العربية


1. عوض، هبة عاطف السيد محمود. (2025) .النصب الإلكتروني في العصر الرقمي .مجلة البحوث الرقمية، 12(1)، 23–47.
2. الاتجاهات الحديثة في الجرائم الإلكترونية عبر مواقع التواصل. (2025). مجلة العلوم الرقمية العربية، 8(2)، 15–38.
3. المسؤولية الجزائية عن جرائم النصب والاحتيال الإلكتروني في الجزائر. (2024). مجلة القانون والعلوم الرقمية، 5(1)، 56–78.
4. آليات القانونية لمكافحة الاحتيال عبر مواقع التواصل الاجتماعي. (2023). مجلة الدراسات القانونية الرقمية، 6(2)، 12–34.
5. الهيئة السعودية للأمن السيبراني. (2023) .تقرير الاحتيال الرقمي في المملكة العربية السعودية .الرياض: وزارة الاتصالات وتقنية المعلومات.
6. القحطاني، محمد بن سعد (2022) الجرائم الإلكترونية وأساليب الوقاية منها .الرياض: دار الفكر.
7. عبدالله، أحمد حسن (2021) .الاحتيال الإلكتروني في المجتمع العربي: الأسباب والآثار .القاهرة: دار النهضة العربية.
8. الزهراني، فهد بن علي (2021). الثقافة الرقمية وأمن المعلومات .جدة: دار حافظ.
9. العنزي، خالد بن محمد (2020) .الوعي الرقمي ودوره في الحد من الجرائم الإلكترونية .الكويت: مكتبة الفلاح.
10. السلمي، ناصر بن حسين (2020) .التفاعل الاجتماعي في الفضاء الرقمي .الرياض: مكتبة العبيكان.
11. قانون مكافحة جرائم المعلوماتية السوداني لسنة 2018 تعديل لسنة 2020م.
12. الحميدي، عبدالله بن صالح (2019) .علم النفس الاجتماعي والسلوك الرقمي .عمّان: دار المسيرة.


### ثانياً: المراجع الأجنبية


1. Pitchan, T., Lee, J., & Rahman, M. (2025). *Cyber Fraud and Digital Awareness: A Systematic Review*. Malaysian Journal of Computing, 22(3), 45–67.
2. Mouncey, P., & Ciobotaru, A. (2025). *Phishing Awareness on Social Media: Experimental Evidence*. Computers & Security, 118, 102789.
3. Pew Research Center. (2025). *Online Scams and Attacks in America Today*. Washington, D.C.: Pew Research Center.
4. Acharya, S., Kumar, P., & Zhao, L. (2024). *Fraudulent Donation Scams on Social Media Platforms*. arXiv preprint arXiv:2412.15621.
5. Jain, A., & Gupta, S. (2020). *Phishing and Cognitive Factors: A Behavioral Analysis*. PMC, National Center for Biotechnology Information. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7252086/
6. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.
7. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

8. Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Perspective. Computers in Human Behavior, 38, 304–312.
9. Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press.
10. Mitnick, K., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.
11. Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A Comparison of Machine Learning Techniques for Phishing Detection. Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit.
12. Jakobsson, M., & Myers, S. (2007). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley.
13. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
14. Stringhini, G., Kruegel, C., & Vigna, G. (2010). Detecting Spammers on Social Networks. Proceedings of the 26th Annual Computer Security Applications Conference.
15. Moore, T., Clayton, R., & Anderson, R. (2012). The Economics of Online Crime. Journal of Economic Perspectives, 26(3), 3–20.
16. Solove, D. J. (2008). Understanding Privacy. Harvard University Press.
17. GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data. Official Journal of the European Union.
18. Choi, H., & Kim, S. (2019). Digital Scams and Social Media. Journal of Information Technology Research, 12(2), 45–60.
19. Solove, D. J., & Schwartz, P. M. (2021). *Information Privacy Law*. New York: Wolters Kluwer.
20. Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Boston: Cengage Learning.
21. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken: Wiley.
22. Stallings, W. (2020). *Network Security Essentials: Applications and Standards*. Boston: Pearson.
23. Brenner, S. W. (2019). *Cybercrime and the Law*. New York: Oxford University Press.
24. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg.
25. Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Chichester: Wiley.