جامعة المنصورة
كليـة الآداب

النصب الإلكتروني في العصر الرقمي
دراسة حالة

إعـــداد

د. هبة عاطف السيد محمود عوض

مدرس بقسم علم الاجتماع

كلية الآداب- جامعة دمياط

مجـلة كلـية الآداب – جامعـة المنصـورة
العدد السادس والسبعون – يناير ٢٠٢٥

النصب الإلكتروني في العصر الرقمي _ دراسة حالة

د. هبة عاطف السيد محمود عوض

مدرس بقسم علم الاجتماع

كلية الآداب– جامعة دمياط

ملخص البحث

إشكالية الدراسة: *بعد أن أصبح التحول الرقمي ضرورة حتمية، هذا أفسح المجال للعديد من الأفراد في ارتكاب جرائم النصب بأشكال ديناميكية تتطور باستمرار كلما تطورت التكنولوجيا.*

هدف الدراسة: *التعرف على مخاطر إدخال الرقمنة على الحياة الاقتصادية، مناقشة كيفية الحماية من جرائم النصب الإلكتروني.*

أهمية الدراسة: *زيادة وعي الأفراد لتجنب الوقوع كضحايا لعمليات النصب الإلكتروني المتسارع في تطوير أنماطه بشكل طردي مع تطور مجتمع المعلومات العالمي.*

الإطار المنهجي: نوع الدراسة: *وصفية تحليلية. تم استخدام: منهج دراسة الحالة، نظرية مثلث الاحتيال، دليل دراسة الحالة على عينة عمدية (٢٠) حالة.*

نتائج الدراسة: *الجُناة معظمهم ذكور، الضحايا معظمهم إناث. علاقة الجُناة بضحاياهم كان في الأغلب تعارف على شبكات التواصل الاجتماعي. طرق النصب الإلكتروني: عروض فرص عمل، عمليات التسوق الإلكتروني، طلب الزواج، رسالة على الموبايل لتحديث البيانات البنكية، الخداع بالفوز بمبلغ مادي. استخدم الجُناة طرق عديدة لكي يكسبوا ثقة ضحاياهم، مثل: الحوار على الخاص، خداع الجاني ضحيته بأن حالته الاقتصادية مرتفعة للغاية، المقابلة وجهًا لوجه، منح الضحية أرباح قبل النصب الإلكتروني لإثبات صدق النية، خلق العلاقات الاجتماعية، تهكير صفحة على شبكة تواصل اجتماعي وإرسال رسائل منها للأفراد الموجودين عليها. الضحايا لم يستردوا أي أموال من الجُناة.*

توصيات الدرسة: عدم الاستجابة المباشرة للأصدقاء على صفحات التواصل الاجتماعي عندما يطلبون تحويل أموال. عدم الرد على الأرقام التي يتم إرسال رسائل منها، مثل: تم إيقاف حساب كارت الفيزا برجاء الاتصال بنا. عدم عرض بيانات الفيزا لأي شخص. الحذر من الدخول على أي Link. تطبيقات التعارف مكان خصب لتواجد النصابون. صياغة وتفعيل القوانين المواكبة للتطور التكنولوجي السريع. عدم اهتزاز الثقة بالنفس مهما حاول الجاني إضعاف الضحية.

كلمات مفتاحية: *النصب الإلكتروني؛ العصر الرقمي؛ الجرائم الإلكترونية؛ الاحتيال؛ شبكات التواصل الاجتماعي*

Abstract:

The problem of the study: After digital transformation became an inevitable necessity, this opened the way for many individuals to commit fraud crimes in dynamic forms constantly evolving as technology develops.

The study aims to identify the risks of introducing digitization into economic life and discuss how to protect against electronic fraud crimes.The study's importance is Increasing individuals' awareness to avoid falling victim to electronic fraud, the patterns of which are rapidly developing in direct proportion to the development of the global information society.

Method: Study type: Descriptive analytical. Used: Case study method, fraud triangle theory, case study guide on a deliberate sample (20) cases.

Results: Most of the perpetrators were males and most of the victims were females. The relationship between the perpetrators and their victims was mostly through social media. Electronic fraud methods: job offers, online shopping, marriage requests, mobile messages to update bank data, and deception of winning a sum of money. The perpetrators used many methods to gain the trust of their victims, such as private conversation, deceiving the perpetrator's victim that his economic status is very high, face-to-face meetings, giving the victim profits before the electronic fraud to prove the sincerity of intentions, creating social relationships, hacking a page on a social network and sending messages from it to the people on it. The victims did not recover any money from the perpetrators.

Recommendations: Do not respond directly to friends on social media pages when they ask to transfer money. Do not respond to numbers from which messages are sent, such as Your Visa card account has been suspended, please get in touch with us. Do not display Visa information to anyone. Be careful when entering any link. Dating applications are a fertile ground for scammers. Formulate and implement laws that keep pace with rapid technological development. Do not shake self-confidence no matter how much the perpetrator tries to weaken the victim.

Keywords: Electronic fraud; Digital age; Electronic crimes; Scam; Social media

مقدمـــة :

مما لا شك فيه أن ما أحدثته الثورة الرقمية يُعد طفره بكل ما تحمله الكلمة من معنى، وبالتأكيد فقد انعكس ذلك على علاقاتنا وسلوكياتنا بل حدث غزو لكل حياتنا(١). حتى أنه لا يستطيع أحد الآن انكار أن استخدام الإنترنت خاصة شبكات التواصل الاجتماعي قد وصل إلى حد (الإدمان) بالمعنى الحرفي للكلمة، أي هناك تشابه بين قضاء الساعات الطويلة جدًا في تصفح تلك المواقع وبين إدمان المُخدرات والهروين وأي مؤثرات عقلية أخرى. ذلك يرجع إلى أن تلك الشبكات تؤثر على إفراز مادة الدوبامين Dopamine المسئولة عن الشعور بالسعادة والمتعة بعد الحصول على Like أو Follow مثلًا، وبمجرد محاولة البُعد عن تلك الشبكات يؤدي ذلك إلى شعور الفرد بالضيق والاكتئاب، مما قد يستدعى الأمر أحيانًا إلى العلاج الطبي الفوري(٢).

وجدير بالذِكر أن تطور الإنترنت قد أدى إلى تطور التجارة الإلكترونية، مما ساعد في ظهور بيئة أعمال ديناميكية تتم فيها التعاملات دون تفاعلات وجهًا لوجه، سرعان ما أدى هذا إلى أن أصبح الإنترنت هو المحطة الأولى للأشخاص لإتخاذ قرار بشأن شراء الخدمات والمنتجات، وبذلك ساهم هذا في زيادة حجم المعاملات مما ساعد في ظهور العديد من أنظمة الدفع الإلكتروني، مما أدى إلى نموًا هائلًا في سوق السلع الرقمية(٣). أنظمة الدفع الإلكتروني هذه تعني استخدام بدائل نقدية مثل بطاقات الخصم وبطاقات الائتمان وتحويل الأموال إلكترونيًا فهي تقدم خدمات مصرفية عبر الإنترنت لإتمام المعاملات المالية، أي أنها وسيلة يمكن من خلالها ممارسة الأعمال المصرفية عن طريق التعامل باستخدام العمليات الآلية

---

(١) محمد جبريل جبريل: ٢٠٢٣، الإطار التشريعي لمواجهة الثورة الرقمية من الوجهة الجنائية دراسة تحليلية مقارنة، مجلة الدراسات القانونية والاقتصادية_ مجلد٩ عدد٣، ص١٦٦٧. 10.21608/jdl.2023.230278.1201

(٢) يُسرية علي أمان آل جميل: ٢٠٢٣، تحديات استخدام وسائل التواصل الاجتماعي الحديثة على مؤسسة الأسرة في القرن الحادي والعشرين– دراسة وصفية، مجلة العلوم الإنسانية والإجتماعية_ مجلد٧ عدد٩، ص٩١. https://doi.org/10.26389/AJSRP.L060623

(3) Lina Fernandes: 2013, Fraud electronic payment transactions: threats and countermeasures, Asia Pacific Journal of Marketing & Management Review _ Vol.2 (3), p. 23. https://www.researchgate.net/profile/Mohamed-Mourad-Lafifi/post/Is-it-possible-to-help-me-with-similar-sources-or-research-for-the-purpose-of-completing-my-research-projects-on-the-development-of-electronic-paymen/attachment/5cb7642b3843b01b9b9abf38/AS%3A748730219257856%401555522603426/download/FRAUD+IN+ELECTRONIC+PAYMENT+TRANSACTIONS+_+THREATS+AND+COUNTERMEASURES.pdf

والأجهزة الإلكترونية مثل أجهزة الكمبيوتر الشخصية والهواتف وأجهزة الفاكس والإنترنت والبطاقات والقنوات الإلكترونية الأخرى(٤).

فيمكن النظر إلى الخدمات المصرفية الإلكترونية بإعتبارها امتدادًا للبنوك المادية القائمة، فتقوم بإستخدام أجهزة الكمبيوتر لإسترداد ومعالجة البيانات المصرفية ثم بدء المعاملات بشكل مباشر وعن بُعد مع البنك عبر شبكات الاتصال. ومن مميزاتها أنها توفر الخدمات للعملاء في أي وقت وأي مكان، وتعالج تحديات التكامل الإداري المعقدة(٥).

فإنتشار استخدام الإنترنت والأجهزة الذكية أدى إلى تحول إجراء الكثير من المعاملات التجارية في العالم الافتراضي بدلًا من العالم الفعلي، وعلى الرغم من أن ذلك يُعد تطورًا كبيرًا إلا أنه لم يخلو من العديد من التحديات والمخاطر التي أصبحت تهدد أمان المستهلكين عبر تلك البيئة الإلكترونية(٦). فتحوّل الموبايل الشخصي من نطاق الكماليات إلى نطاق الأساسيات، أدى إلى امتلاكه لدى فئة كبيرة من الأفراد قليلي بل عديمي الخبرة في حماية أنفسهم من مجرمي الإنترنت.

وعلى الرغم من أن النصب الإلكتروني والتصيد الاحتيالي ليس جديدًا، فقد أصبح تهديدًا متزايدًا للأمن السيبراني(٧)، فقد رفعت التقنية الحديثة من قوة الأشخاص في ارتكاب الجرائم الإلكترونية باحترافية مخطط لها، وللأسف شكل ذلك خطورة أمنية معقدة تهدد المجتمعات بسبب خطورتها الإجرامية، فقد تعرض العديد من الأشخاص في الآونة الأخيرة للنصب الإلكتروني، الذي لا يتضرر منه المجني عليه فقط بل

(4) OGBONNA, Kelechukwu Stanley & OKARO, Celestine & IGWE, Elizabeth Ihuoma: 2019, Electronic fraud and credit facilitation of banks in Nigeria, Journal of Accounting Information and Innovation _ Vol.5 _ No.10. https://www.researchgate.net/profile/Kelechukwu-Ogbonna/publication/336903627_ELECTRONIC_FRAUD_AND_CREDIT_FACILITATION_OF_BANKS_IN_NIGERIA/links/5dba18534585151435d615b6/ELECTRONIC-FRAUD-AND-CREDIT-FACILITATION-OF-BANKS-IN-NIGERIA.pdf

(5) Emad Abu-Shanab, Salam Matalqa: 2015, Security and Fraud Issues of E-banking, International Journal of Computer Networks and Applications _ Volume 2, Issue 4 _ EverScience Publications, p. 180. https://d1wqtxts1xzle7.cloudfront.net/53498558/Abu-Shanab___Matalqa_2015-libre.pdf?1497418633=&response-content-disposition=inline%3B+filename%3DSecurity_and_Fraud_Issues_of_E_banking.pdf&Expires=1722432407&Signature=FQtislwcVY9yU~4DJJ-JXdbJrZPiXAEzMcSWITDPaE84k~a-NTgLtT7U9Po69q9dZJ7gA2H8IbfTWFqhqDrWdjQriLSbwr2HJscxXtpBlYn3jCr0vqTEkHksHsa19JypwYy0kQXuvbl9pVcIZki0gzt3RuZZVVBJAy2rcpej68JoPDmFMlY5v3PhvWm~JKNPxXvemPmD52pjmp8C2TMgWLJZK5R8OJEjtH7ck3SXPxMAFV815sW~CjoO-mSmQQ~7iAtJGeYRJcugkXZJ8TMbbtNFyFQ38bC-73XeKAcLM6mWzQVeZDuvlILzJndnoeur5pN6TloB~SH5Tnm8xCEL1g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

(٦) يحيى إبراهيم دهشان: ٢٠٢٤، الحماية الجنائية للمستهلك الإلكتروني، الدوريات المصرية. https://journals.ekb.eg/article_352592_0.html

(7) María M. Moreno-Fernandez, Fernando Blanco, Pablo Garaizar, Helena Matute: 2017, Fishing for phishers _ Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud, Computers in Human Behavior _ Volume 69 _ Elsevier, p. 421. https://doi.org/10.1016/j.chb.2016.12.044

أيضًا المجتمع والدولة[٨]. وذلك لأن النصب الإلكتروني يمكن تشبيهه بمرض مُعدٍ لا يؤدي إلى تعطيل الجهاز المصرفي فحسب، بل إن آثاره محسوسة في كل اقتصادات القطاعات الأخرى، حيث أن له تأثير سلبي على سيولة البنوك فيبدأ أدائها في التدهور، مما يكون له أكبر الأثر على المجتمع لأن أدوار المؤسسة البنكية يُمكن اعتبارها من الأجزاء الأكثر أهمية حيث يُمكن الإشارة إليها بالجهاز العصبي المركزي للمجتمع[٩].

أولًا: إشكالية الدراسة

بعد أن أصبح التحول الرقمي ضرورة حتمية في شتى مجالات الحياة، كان بديهيًا أن يقتحم هذا التحول الحياة البشرية بمختلف صورها خاصة: (الجوانب الاجتماعية) ذلك لأن أي إنسان في الغالب لا يستطيع الاستغناء طوال يومه عن علاقاته مع الآخرين، وأيضًا (الجوانب الاقتصادية) التي تتمثل في عمليات الشراء والبيع اللازمة لإستمرار التفاعل الإنساني. وللأسف هذا أفسح المجال للعديد من الأفراد –ليس فقط النصابون المحترفون– في ارتكاب جرائم النصب بكل سهولة، بل بأشكال ديناميكية تتطور باستمرار كلما تطورت التكنولوچيا.

وحتى الدول المتقدمة مثل الولايات المتحدة قد تأثرت سلبًا بعمليات الاحتيال الإلكتروني، ففي عام ٢٠١٦ قد تأثر (١٥.٤) مليون مستهلك أمريكي بإحتيالات الهوية بمبلغ (١٦ مليار دولار أمريكي)، وكان عدد الضحايا أعلى بنسبة (١٦%) مقارنة بعام ٢٠١٥[١٠].

ووفقًا لإحصائيات جمعية مكافحة الاحتيال في الاتصالات –في عام ٢٠١٩ وحْدُه– فقد تسبب الاحتيال في خسارة عالمية بلغت ٢٨.٣ مليار دولار أمريكي، والأموال التي تتمكن وكالات إنفاذ القانون من استردادها في مثل هذه الحالات محدودة للغاية. فقد أفاد أحد البنوك التايوانية أن هذه الطريقة القائمة على القواعد تنتج معدل استدعاء ضعيف (٥.٥٦٪) فقط، ومعدل دقة (٤٠٪). حيث تتبنى العديد من

(٨) عبدالوهاب عبدالكريم محمد المبارك: ٢٠٢٣، إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك، المجلة القانونية_ مجلد١٥ عدد٨_ كلية الحقوق فرع الخرطوم جامعة القاهرة، ص١٩٢١. 10.21608/JLAW.2023.286561

(9) Folowosele Folarin Akinwale, Ikpefan Ochei Ailemen, Isibor Areghan: 2022, Electronic fraud: an emerging cause of bank failure in Nigerian deposit money banks, Journal of Money Laundering Control _ Volume 25 Issue 1 _ Emerald Insight. https://doi.org/10.1108/JMLC-01-2021-0009

(10) Zahoor Ahmed Soomro, Javed Ahmed, Mahmood Hussain Shah, Khalil Khoumbati: 2019, Investigating identity fraud management practices in e-tail sector: a systematic review, Journal of Enterprise Information Management _ Volume 32 Issue 2 _ Emerald Publishing Limited, p.302. https://www.emerald.com/insight/content/doi/10.1108/jeim-06-2018-0110/full/html

البنوك التجارية قاعدة عامة لتطوير أنظمة الكشف الآلي للاحتيال الإلكتروني، تشكل مجموعة من القواعد أو المرشحات لاكتشاف الحسابات الاحتيالية الحقيقية من قائمة طويلة من الأنشطة المشبوهة التي تم إنشاؤها بناءً على ملاحظات أو اقتراحات سابقة من وكالات الشرطة(١١).

وتتضح مشكلة الاحتيال المالي أيضًا من أرقام تقرير مسح لعام ٢٠٢٢ الذي يكشف أن ٥٦% من الشركات على مستوى العالم وقعت ضحية لشكل من أشكال الاحتيال، وفي أمريكا اللاتينية تعرضت ٣٢% من الشركات للاحتيال. وتتوافق هذه الإحصائيات المزعجة مع النتائج التي توصلت إليها إحدى الشركات، والتي تشير إلى أن ٨٣% من المديرين التنفيذيين الذين شملهم الاستطلاع أفادوا بأنهم تعرضوا لهجمات إلكترونية. وتكشف نتائج هذا المسح عن المخاطر الأعلى للاحتيال المالي التي تواجهها الشركات في أمريكا اللاتينية والولايات المتحدة وكندا. وفي هذا السياق، فقدت الأساليب والتقنيات التقليدية، فضلاً عن الأساليب اليدوية، أهميتها وفعاليتها لأنها لا تستطيع معالجة تعقيد وحجم المعلومات المتضمنة في الكشف عن الاحتيال المالي بشكل فعال(١٢).

بهذا يتلخص التساؤل الرئيس لهذه الدراسة في: ما أبعاد النصب الإلكتروني في العصر الرقمي؟. ذلك مع محاولة وضع تصور للحماية من نصابين الإنترنت وتحقيق الأمن السيبراني.

ثانيًا: أهداف الدراسة

١) دراسة مخاطر إدخال الرقمنة على الحياة الاقتصادية.
٢) التعرف على الأشكال الحديثة لعمليات النصب الإلكتروني.
٣) مناقشة كيفية الحماية من جرائم النصب الإلكتروني.

ثالثًا: أهمية الدراسة

١) الأهمية النظرية

تحاول الدراسة صياغة سطرًا إضافيًا للبحوث في مجال النصب الإلكتروني؛ يكون ملخصًا يجمع أشهر أشكال التعدي بالنصب على الأفراد في مجتمعهم الرقمي.

(11) Yen-Wu Ti, Yu-Yen Hsin, Tian-Shyr Dai, Ming-Chuan Huang, Liang-Chih Liu: 2022, Feature generation and contribution comparison for electronic fraud detection, Scientific reports. https://doi.org/10.1038/s41598-022-22130-2

(12) Ludivia Hernandez Aros, Luisa Ximena Bustamante Molano, Fernando Gutierrez-Portela, John Johver Moreno Hernandez, Mario Samuel Rodríguez Barrero: 2024, Financial fraud detection through the application of machine learning techniques: a literature review, humanities and social sciences communications.
https://doi.org/10.1057/s41599-024-03606-0

٢) الأهمية التطبيقية "الميدانية"

زيادة وعي الأفراد لتجنب الوقوع كضحايا لعمليات النصب الإلكتروني المتسارع في تطوير أنماطه بشكل طردي مع تطور مجتمع المعلومات العالمي. ومثالًا لهذا التطور الذي حدث في الأيام القليلة السابقة، أن تم إرسال رسالة صوتية باللغة العربية لعدد كبير جدًا من الأفراد من رقم موبايل بصوت فتاة تُعَرِف نفسها بأنها تتبع شركة تسويق إلكتروني، ولديها عرض عمل سهل في وقت الفراغ عبارة عن عمل إعجاب لمقاطع فيديو تيك توك للتجار، وتدفع الشركة ٢٠ جنيهًا مصريًا لكل مهمة، أي يمكنك كسب ما يصل إلى ٢٥٠٠- ٨٠٠٠ جنيه مصري يوميًا. هل أنت مهتم بالعمل معنا؟ أخبرنا وسنرشدك، يمكن أن يساعدك هذا في كسب المزيد من المال!. عند الرد عليهم بأن الشخص مهتم؛ تصل رسالة مكتوبة تقول قبل أن نبدأ يرجى ملء هذا: كم عمرك؟ ما هي وظيفتك؟ هل يمكنني أن أعرف إذا كان لديكم تطبيق تيليجرام؟ ندفع عبر فودافون أو ET Cash أو Orange Cash أو أي محفظة إلكترونية أخرى، هل لديك أي منها، سيدي/ سيدتي؟.

ومعلوم أن تطبيق تيك توك قد اكتسب شهرة كبيرة في الآونة الأخيرة بين الشباب، وبهذا فهؤلاء النصابون يعملون دائمًا على مواكبة كل جديد حتى تكون فرصتهم أكبر في الإيقاع بالضحايا.

رابعًا: تساؤلات الدراسة

س١: كيف يتم التعرض للنصب الإلكتروني في العصر الرقمي؟

س٢: ما الآثار الاجتماعية للنصب الإلكتروني؟

س٣: ما التدابير الأمنية لتجنب الوقوع في فخ النصب الإلكتروني؟

خامسًا: مفاهيم الدراسة

١) النصب الإلكتروني

هو جريمة يكون الغرض منها الإستيلاء على الأموال بوسائل غير قانونية، ويتسبب في المزيد من الخسائر الآن مقارنة بالماضي، كما يُمكن تعريفه على أنه استخدام مهنة المرء للإثراء الشخصي من خلال سوء الإستخدام المتعمد أو سوء تطبيق موارد أو أصول المنظمة التي توظفه[١٣].

(13) Aisha Abdallah, Mohd Aizaini Maarof, Anazida Zainal: 2016, Fraud detection system: A survey, Journal of Network and Computer Applications _ Volume 68 _ Elsevier. https://doi.org/10.1016/j.jnca.2016.04.007

أيضًا هو مُخطط يهدف إلى خداع شخص أو أشخاص للحصول على مبلغ معين من المال أو السلع[١٤]، أي أنه خرق للثقة يتسبب في مكسب غير مشروع لشخص وخسارة غير مشروعة للآخر، وربما يتم استخدام التزوير المتعمد الذي يتطلب غالبًا بعض الخبرة الفنية من أجل الحصول على أموال من البنك بطريقة احتيالية[١٥]. وبذلك يمكن اعتباره الإساءة المرئية للخدمات المصرفية الإلكترونية[١٦]. أي أن النصب الإلكتروني عبارة عن حدوث خسارة لأحد الطرفين نتيجة لإحتيال الطرف الآخر في سياق المعاملات بين البائعين والمستهلكين عبر الإنترنت. وهذا يحدث بسبب الثقة المسبقة من المشتري في البائع أو العكس، حيث أن أحدهما يقبل ضعف العلاقة على الإنترنت على أساس التوقعات الإيجابية لنزاهة الطرف الآخر وإحسانه. وبهذا فإن النصب الإلكتروني ربما يحدث أيضًا للبائعين بسبب احتيال المشترون الذين يحتالون على البائعين كأن يدَعوا بأنهم لم يستلموا المنتج أو الخدمة[١٧].

يُمكن تصنيف النصب الإلكتروني إلى نوعين؛ النصب المباشر الذي قد يشتمل على الاحتيال على بطاقات الإئتمان أو اختلاس يقوم به موظفين وغسيل الأموال والهجوم على الأموال، النصب غير المباشر الذي قد يشتمل على التصيد الاحتيالي من تزييف وقرصنة وفيروسات والبريد العشوائي والبرمجيات الخبيثة[١٨].

وبذلك فإن حدوث النصب في بيئة الأعمال الإلكترونية عن طريق الاختراق الأمني والتلاعب بأصحاب الحسابات من قِبل المحتالين، قد أصبح مصدر قلق كبير لمقدمي الخدمات ومستخدمي منصات الدفع الإلكترونية. وبهذا فعلى الرغم من أن استخدام الإنترنت قد أدى إلى تسهيل وتمكين أنشطة العمليات التجارية بين العملاء والموردين التجاريين سواء كان ذلك في خدمات مصرفية وبيع السلع والخدمات عبر

(14) Damaris Karimi Mwabu: 2013, Factors influencing electronic fraud in the banking industry in Kenya:a case of Kenya commercial bank central region, College of Humanities and Social Sciences _ Faculty of Education _ University of Nairobi, p. 9. http://erepository.uonbi.ac.ke/handle/11295/60487

(15) Adaora Immaculata Muoghalu, Jisike Jude Okonkwo, Amalachukwu Chijindu Ananwude: 2018, Effect of electronic banking related fraud on deposit money banks financial performance in Nigeria, Discovery Publication _ 54 (276), p. 497. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305555

(16) Amaefule I.A, Onu F.U: 2019, Prevalence of Electronic Fraud in Nigeria Banking System, International Journal of Computer Trends and Technology _ Volume 67 Issue 3, p. 78. https://www.researchgate.net/profile/I-Amaefule/publication/334053572_Prevalence_of_Electronic_Fraud_in_Nigeria_Banking_System/links/5efee28692851c52d6137dee/Prevalence-of-Electronic-Fraud-in-Nigeria-Banking-System.pdf

(17) Yue Guo, Yongchuan Bao, Barnes J. Stuart, Khuong Le-Nguyen: 2017, To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce, Wiley online library _ Volume 28 Issue 2. https://doi.org/10.1111/isj.12144

(18) Shewangu Dzomira:2014, Electronic fraud (cyber fraud) risk in the banking industry _ Zimbabwe, Risk governance & control: financial markets & institutions _ Volume 4 _ Issue 2, p. 17. https://www.researchgate.net/profile/Shewangu-Dzomira-2/publication/282281593_Electronic_fraud_cyber_fraud_risk_in_the_banking_industry_Zimbabwe/links/560a58a908ae576ce63fc422/Electronic-fraud-cyber-fraud-risk-in-the-banking-industry-Zimbabwe.pdf

الإنترنت، بل أنه ربما يكون أقل من حيث التكلفة، إلا أن الخوف من فقدان الموارد المالية قد يكون سببًا لعدم الاعتماد الكامل على استخدام القنوات الإلكترونية(١٩).

فقد اجتذبت الزيادة في أنشطة الدفع الإلكتروني مستوى مرتفعًا وغير مسبوق من الاحتيال الإلكتروني في نظام الخدمات المصرفية في جميع أنحاء العالم، هذا الاحتيال الذي يُعَد عائقًا كبيرًا أمام النجاح والاستقرار لأنظمة الدفع والتحصيل حيث أدى إلى محنة العديد من البنوك، وللأسف فإن هذا الاحتيال في ارتفاع على الرغم من الإجراءات غير المسبوقة لتقليل حالات الاحتيال الإلكتروني، لأن المحتالين يبتكرون بإستمرار طرقًا استراتيجية جديدة لإرتكاب عمليات الاحتيال. ولعل العامل المتناقض هو أنه على الرغم من الضرر الهائل الذي ألحقه الاحتيال الإلكتروني بإقتصاد المجتمع إلا أن عملية الإدانة والعقاب ضعيفة نسبيًا، وذلك قد شجع مرتكبي جرائم النصب الإلكتروني من الاستمرار في أنشطتهم الشائنة(٢٠).

التعريف الإجرائي للنصب الإلكتروني: الاستيلاء على أموال الغير بطرق غير مشروعه، وذلك يكون باستخدام وسيلة تكنولوچية.

٢) العصر الرقمي

يُعرَف بأنه ذلك الوقت الذي أصبح فيه للإنسان القدرة على تحويل المعلومات إلى صورة رقمية، يتم إنتقالها خلال شبكة الإنترنت بإستخدام أجهزة إلكترونية مثل الهاتف والكمبيوتر، حيث أنها تُمَكِن من تخزين وتوزيع كم هائل من تلك المعلومات الرقمية بشكل مستمر(٢١).

يعود بزوغ فجر العصر الرقمي إلى اختراع مهم في عام ١٦٧٩م عندما تم تطوير نظام الأرقام الثنائية القائم على: (٠، ١) هذا النظام هو أساس معالجة المعلومات والبيانات الإلكترونية الحديثة، ثم توالت بعد ذلك اختراعات الحوسبة إلى أن تم اختراع أول كمبيوتر يعمل بشكل صحيح عام ١٩٤١م، ثم تم تطوير

(19) Babatunde Moses Ololade, Mary Kehinde Salawu, Aderemi Daniel Adekanmi: 2020, E-Fraud in Nigerian Banks: Why and How?, Journal of Financial Risk Management _ Vol.9 No.3 _ Scientific Research Publishing. 10.4236/jfrm.2020.93012

(20) Charles Emeka Nwobia, Patrick Anayo Adigwe, Gideon Kasie Ezu, John Nonso Okoye: 2020, Electronic Fraud and Performance of Deposit Money Banks in Nigeria: 2008-2018, International Journal of Business and Management _ Vol. 15 _ No. 6 _ Canadian Center of Science and Education, p. 126. 10.5539/ijbm.v15n6p126

(٢١) راوية عبدالحميد إبراهيم، محمد جابر محمود، رشاد ابوالمجد مصطفى: ٢٠٢٣، العصر الرقمي: مفهومه وخصائصه ومتطلباته وتأثيره على قيم المواطنة، مجلة العلوم التربوية_ كلية التربية بقنا_ جامعة جنوب الوادي_ عدد٥٥ ج١، ص ١٢٠. https://maeq.journals.ekb.eg/article_299655_426478877b90a48f5022b74a041e968b.pdf

الأجهزة بعد ذلك إلى أن أصبحت الآن أصغر وأسرع، واليوم يربط الإنترنت ملايين من تلك الأجهزة في جميع أنحاء العالم(٢٢).

وبذلك فإن العصر الرقمي قد بدأ منذ أواخر القرن العشرين، فبإستخدام نقرة الماوس يستطيع أي شخص أن يصل إلى ملايين البشر في زمن قياسي، هذا العصر أوجد حالة إنسانية وعلمية لا تستطيع فيها العقول إدراك مدى أبعادها أو التنبوء بما ستؤول إليه في المستقبل، حيث أحدث هذا العصر بكل معطياته قدرة هائلة وفائقة في التواصل الإنساني، وأوجد سياقات تفاعل وسَهَل الحياة على البشر(٢٣).

فإنتشار مظاهر العصر الرقمي قد أدى إلى زيادة قدرة البشر على توسيع معارفهم وخبراتهم من خلال استخدام الوسائل الرقمية، التي ساعدت على التعرف على الثقافات المختلفة والمجتمعات المتقدمة ومواكبتها لتحقيق التطور والاستفادة في كافة المجالات(٢٤). حتى أنه أصبح نادرًا أن نجد شخصًا ليس له علاقة بالرقمنة، بل وأصبح يُطلق على الذين لا يعرفون كيفية التعامل مع التقنية الرقمية أنهم الأُميون الرقميون(٢٥).

والمجتمع في هذا العصر يُطلق عليه مجتمع المعلومات أو المجتمع الإلكتروني أو المجتمع الرقمي، ذلك حيث تشكلت فيه صورة جديدة للأنشطة والمعاملات البشرية، فأصبحت المعلومات موردًا اقتصاديًا مهمًا ورأس مال حديثًا وجديدًا(٢٦). وأصبحت القوة بيد من يملك المعرفة والتقنيات الحديثة والبرمجة(٢٧).

---

(٢٢) مفيدة طاير: ٢٠٢٠، مقومات وتحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا وعلوم الإعاقة_ مجلد٢ عدد٤، ص ص ٢٠٠، ٢٠١. 10.21608/SKJE.2020.38254.1003

(٢٣) فايزة عبيد، نريمان حريسي: ٢٠٢٢، الإدارة الإلكترونية ودورها في العصر الرقمي، مذكرات العلوم الإنسانية_ قسم علوم الإعلام والإتصال_ كلية العلوم الإنسانية والاجتماعية_ جامعة العربي التبسي. http//localhost:8080/jspui/handle/123456789/5225

(٢٤) أماني رضا أبوالمعارف سباع: ٢٠٢١، أداء المعلم الجامعي في ضوء متطلبات العصر الرقمي، مجلة العلوم التربوية_ كلية التربية بقنا_ مجلد ٤٦ عدد ٤٦، ص٥٩. 10.21608/maeq.2021.77805.1027

(٢٥) ولاء أسعد عبدالجواد عبدالحليم: ٢٠٢٤، الكتابة الإبداعية في العصر الرقمي "الفرص والتحديات"، المجلة العلمية لكلية الآداب جامعة أسيوط_ مجلد٣١ عدد٨٩، ص٦٣١. 10.21608/AAKJ.2023.249423.1604

(٢٦) محمود موسى زياد: ٢٠٢٤، الفلسفة وتحديات العصر الرقمي، مجلة التطوير العلمي للدراسات والبحوث_ مجلد٥ عدد١٧، ص٣٦١. https://doi.org/10.61212/jsd/196

(٢٧) حملاوي مهتور: ٢٠٢٤، الفلسفة أهميتها ومآلها في العصر الرقمي، مجلة التطوير العلمي للدراسات والبحوث_ مجلد٥ عدد١٨، ص٣٥٥. https://doi.org/10.61212/jsd/222

هذا العصر ظهرت فيه ثقافة المنصات، كمحور غاية في الأهمية في نطاق التفاعلات الاجتماعية الجديدة. ففي ظل تحولات العالم الرقمي تغيرت العديد من التنظيمات الاجتماعية التقليدية، وأصبحت الأنشطة البشرية تتم عن طريق الرقمنة مثل البحث عن شريك عمل أو استهلاك البضائع عن طريق استخدام الحسابات الشخصية على تلك المنصات، التي أصبح لها دور رئيسي في الترويج للذات وللشركات وللسلع والخدمات والترفيه والتواصل بإستخدام الإعلانات على مواقع التواصل الاجتماعي لتحقيق الأرباح التجارية(٢٨).

التعريف الإجرائي للعصر الرقمي: الحياة الحديثة التي ازدادت فيها القدرة على الوصول لمختلف أنواع المعلومات، مع إمكانية توظيفها والإستفادة منها بإستخدام التكنولوچيا الحديثة. وتطبيقًا على الحالات الميدانية؛ فكانت هناك قدرة للنصابون على الوصول إلى معلومات عديدة عن ضحاياهم، تلك المعلومات التي استطاعوا فيما بعد توظيفها والإستفادة منها في صالحهم ضد الضحايا، عن طريق استخدام التكنولوچيا الحديثة أو الأجهزة الإلكترونية بهدف إتمام عملية النصب.

سادسًا: الدراسات السابقة

❖ محور النصب الإلكتروني

١) الإحتيال الإلكتروني من تغيير المفهوم إلى تغيير الحماية_ ٢٠٢٣(٢٩)

تعتبر جرائم الإحتيال والنصب من الجرائم التقليدية التي تقوم على الإستيلاء على أموال منقولة مملوكة عن طريق خداع الضحية وإجبارها على التسليم، وقد تطورت في عصر المعلومات وظهر مصطلح الإحتيال الإلكتروني، حيث تتم الجريمة على المنصات الرقمية بهدف الإستيلاء على أموال الآخرين باستخدام طرق إحتيالية مختلفة. فيجب إلقاء الضوء على ضرورة معالجة الإحتيال الإلكتروني في الأطر القانونية، ومواجهة التحديات التي تفرضها المنصات الإفتراضية، سعيًا لمعرفة ما إذا كان الإعتماد على النصوص القانونية التقليدية كافيًا أم أن التدابير الجديدة ضرورية للحماية الفعالة من هذه الجرائم المتخصصة. تم استخدام المنهج التحليلي من خلال تحليل النصوص التي ساهمت في معالجة الاحتيال

(٢٨) وليم هوسلي، ترجمة: وليد رشاد زكي: ٢٠٢١، المجتمع في العصر الرقمي: منظور تفاعلي، المجلة المصرية للعلوم الاجتماعيـــة والســـلوكية_ مؤسســـة تواصـــل للدراســـات والتوعيـــة الثقافيـــة، ص ص ٢٠٨، ٢٠٩.
https://ejsbs.journals.ekb.eg/article_203573_f918e1dc44078e1da167060b11fed84c.pdf

(29) Ghazioui Hinda: 2023, Electronic fraud from changing the concept to changing the protection, International journal of legal and political research _ Volume 7 Issue 3, p. p. 7: 21. https://www.asjp.cerist.dz/en/downArticle/473/7/3/237838

الإلكتروني، بالإضافة إلى المنهج الوصفي. وعليه جاءت هذه الدراسة لتسليط الضوء على تحول مفهوم الإحتيال الإلكتروني مما أدى إلى ضرورة إعادة تعريف آليات الحماية منه.

٢) علاقة مواقع التواصل الاجتماعي بالنصب والاحتيال من وجهة نظر طلبة الجامعين "دراسة ميدانية على عينة من طلبة علوم الاعلام والاتصال جامعة قاصدي مرباح ورقلة"_ ٢٠٢٣[٣٠]

يتلخص هدف الدراسة في الوصول إلى علاقة شبكات التواصل الاجتماعي بالنصب والاحتيال من وجهة نظر طلبة علوم الإعلام والاتصال. تم استخدام المنهج الوصفي واستمارة الاستبيان على عينة قصدية قوامها (٥٠) طالب. النتائج: انستجرام من أشهر المواقع التي يقع فيها النصب والاحتيال الإلكتروني وهذا يعود إلى الخدمات المتاحة عليه، النصب والاحتيال تقوم به مؤسسات وهمية لخداع المستخدمين بأساليب متنوعة، النصب والاحتيال يتم عن طريق انتحال شخصيات مزيفة، أكبر دوافع النصب هو الاستحواذ على الحسابات المصرفية، معرفتك لمن تتعامل معه سوف تحميك من النصب والاحتيال، قام نصابون بالاستيلاء على بيانات شخصية لأفراد وتم استخدامها في أغراض مشبوهة، قد يلجأ المحتالين إلى طريقة الخداع بوجود جمعيات أهلية لكسب تعاون الأفراد والنصب عليهم.

٣) نموذج للتنبؤ بتهديدات الاحتيال الإلكتروني على قنوات دفع إلكترونية مختارة باستخدام الانحدار الخطي_ ٢٠٢٢[٣١]

يعد الاحتيال الإلكتروني مشكلة أصبحت مصدر قلق للشركات بجميع أحجامها، ذلك لأنه يؤدي إلى زيادة هامش الخسارة حيث يتجاوز المجرمون الآن المؤسسات التقليدية وأصبحوا يستهدفون الشركات التي لها تواجد عبر الإنترنت وطرق دفع إلكترونية. الغرض من هذه الورقة البحثية هو اقتراح نموذج يُمَكِن صناع القرار من استخدامه لتوقع التهديدات وتوفير التدابير الوقائية وحساب نسبة الربح في الدخل بعد تنفيذ التدابير الوقائية، وسيساعد ذلك في حماية الشركات والمستهلكين من الاحتيال الإلكتروني أثناء استخدام قنوات الدفع الإلكترونية المحددة. يقدم هذا النموذج لصناع القرار في البنوك وشركات التكنولوجيا المالية بيانات تاريخية عن حجم الاحتيال في الدفع الإلكتروني على كل قناة من القنوات المختارة، وسوف يسمح

(٣٠) بن قفة سمراء، نوي نور الهدى: ٢٠٢٣، علاقة مواقع التواصل الاجتماعي بالنصب والاحتيال من وجهة نظر طلبة الجامعين "دراسة ميدانية على عينة من طلبة علوم الاعلام والاتصال جامعة قاصدي مرباح ورقلة"، جامعة قاصدي مرباح ورقلة_ كلية العلوم الإنسانية والاجتماعية_ قسم علوم الإعلام والاتصال. https://dspace.univ-ouargla.dz/jspui/handle/123456789/34553

(31) Olubunmi Alabi, Amos David: 2022, Model for forecasting electronic fraud threats on selected electronic payment channels using linear regression, International Journal of Information Technology _ Volume 14 _ Springer Nature, p. p. 2657: 2666. https://doi.org/10.1007/s41870-022-00939-4

النموذج لصناع القرار بالتنبؤ بالاحتيال الإلكتروني على قنوات الدفع الإلكتروني المختلفة، تم الحصول على البيانات المستخدمة من البنك المركزي النيجيري، يقدم النموذج طرقًا لتنفيذ التدابير الوقائية بالإضافة إلى زيادة مئوية في الدخل بعد التنفيذ، ستساعد هذه النتائج في تقليل الاحتيال في الدفع الإلكتروني وزيادة اعتماد العملاء على المدفوعات الإلكترونية.

٤) دراسة استقصائية حول إدارة مخاطر الاحتيال الرقمي من خلال نظام إدارة الحالات التلقائي_ ٢٠٢١[٣٢]

في هذا العصر الرقمي تم غسل كميات هائلة من الأموال عبر عمليات الإحتيال الإلكترونية، حيث يحدث النصب الإلكتروني في إطار معاملات الدفع الإلكترونية التي يقوم بها مستخدموا بطاقات الإئتمان/ الخصم. من المرجح أن هذا الاحتيال يحدث بسبب البنية التحتية الحالية التي لا تحتوي إلا على قاعدة بيانات قديمة. تقدم تلك الورقة البحثية نظرة عامة مُقترحَة لتطوير نظام وقاية آلي لأي مؤسسة مالية لحمايتها من أي هجمات احتيالية، وذلك عن طريق نظام إدارة الحالات الآلي لمراقبة سلوك المستخدِمين من خلال تجنُب الاتصال غير المرغوب فيه، يُمكن لهذا النظام التنبؤ بالإحتيال الرقمي بإستخدام قاعدة بيانات قديمة مُحَدَثة، وذلك من خلال التحليل القائم على المحتوى.

٥) أبعاد الاحتيال الإلكتروني وحوكمة الثقة في النظام البيئي غير النقدي في نيجيريا_ ٢٠٢٠[٣٣]

تؤكد تلك الدراسة أن النتيجة السلبية للسياسة غير النقدية الناشئة في نيجيريا هي الاحتيال المصرفي الإلكتروني المستمر، كما أن حدوث الاحتيال في أي مجال مالي يشير بالتأكيد إلى انعدام الأمن والثغرات التي يستغلها المحتالون. وهذا يؤكد أهمية خلق الثقة في الخدمات المصرفية الإلكترونية في اقتصاد عابر غير نقدي مثل نيجيريا. على هذه الخلفية، قامت الدراسة بالتحقيق في الاحتيال المصرفي الإلكتروني عند استخدام الخدمات المصرفية الإلكترونية، وباستخدام الأساليب النوعية (المقابلات المتعمقة والمقابلات مع المخبرين الرئيسيين) لجمع البيانات، تم اختيار ٣٠ مشاركًا بشكل مقصود، وفي بعض الحالات تم الوصول إليهم من خلال أساليب كرة الثلج والإحالة. وأظهرت النتائج الأبعاد الداخلية والخارجية والتعاونية

(32) Wang Haoxiang, S. Smys: 2021, A Survey on Digital Fraud Risk Control Management by Automatic Case Management System, Journal of Electrical Engineering and Automation _ Vol.03 No.01. https://web.archive.org/web/20210511004002id_/https://irojournals.com/iroeea/V3/I1/01.pdf

(33) Oludayo Tade, Oluwatosin Adeniyi: 2020, Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem, International Journal of Offender Therapy and Comparative Criminology _ Volume 64 Issue 16 _ Sage Journals. https://doi.org/10.1177/0306624X20928028

للاحتيال الإلكتروني، وأن البنوك تتبنى آليات أمنية مثل إرسال رسائل تنبيه للاحتيال إلى العملاء، أيضًا يتم فضح الموظفين المتورطين وإقالتهم كتدابير داخل البنك لضمان ثقة العملاء في النظام البيئي المالي المتطور.

٦) تقنيات مكافحة الاحتيال في الخدمات المصرفية الإلكترونية_ ٢٠١٩[٣٤]

تتناول تلك الورقة مزايا الخدمات المصرفية الإلكترونية والظواهر السلبية المحتملة "المخاطر" التي قد تنشأ في عملية استخدام الخدمات المصرفية. تم إيلاء اهتمام خاص لأسباب الاحتيال في عمل الخدمات المصرفية الإلكترونية، فضلاً عن أهداف تعديات المحتالين في هذا المجال. تمت دراسة الأساس القانوني لحل قضايا مكافحة الاحتيال في مجال الخدمات المصرفية الإلكترونية فيما يتعلق بالمعايير الدولية في تجربة الاتحاد الأوروبي. تم تحديد الجوانب الإشكالية المتعلقة باستعادة الأموال المفقودة لأحد عملاء البنك نتيجة الإحتيال من قِبل أطراف ثالثة.

٧) الإحتيال على ماكينات الصرف الآلي في جنوب غرب نيجيريا: أنماط الضحايا واستراتيجيات الإحتيال والوقاية من الإحتيال_ ٢٠١٧[٣٥]

بحثت الدراسة العوامل التي تجعل الأفراد عرضة للإحتيال على ماكينات الصرف الآلي. وبإستخدام أسلوب المقابلة المتعمقة، تم جمع البيانات من ٢٠ ضحية. أظهرت النتائج أن الضحايا كانوا صغارًا وكبارًا وشملوا الذكور والإناث، كان المحتالون عادةً عشاقًا وأصدقاء وأقارب وأحيانًا أطفال الضحايا. تم الإبلاغ عن استنساخ البطاقات وتبادل البطاقات والإعتداءات الجسدية على ماكينات الصرف الآلي كتكتيكات للاحتيال، وشملت عوامل الضعف: الأمية وسوء الحالة الصحية. وكوسيلة للتخفيف من الاحتيال، وُجد أن البنوك استخدمت مجموعة متنوعة من الاستراتيجيات مثل: تحسينات في رعاية الموظفين، وفرض عقوبات صارمة على الموظفين المذنبين، وتعزيز الوعي بالاحتيال من خلال تنبيهات العملاء.

٨) الرصد الإحصائي للإحتيال الإلكتروني في البنوك النيجيرية_ ٢٠١٦[٣٦]

(34) Daria Kibets, Olena Lepei, Oleksii Prokopenko, Alina Chorna, Mykola Shelukhin: 2019, Anti-Fraud Technologies in E-Banking, Journal of legal, ethical and regulatory issues _ Volume 22 special Issue 2 _ Hein on line. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jnlolletl22&div=168&id=&page=

(35) Tade, Oludayo & Adeniyi, Oluwatosin: 2017, Automated teller machine fraud in south-west Nigeria: Victim typologies, victimisation strategies and fraud prevention, Journal of Payments Strategy & Systems _ Volume 11 Number 1 _ Henry Stewart Publications, p. p. 86: 92. https://www.ingentaconnect.com/content/hsp/jpss/2017/00000011/00000001/art00011

منذ فترة من الزمن، أصبح المستهلكون يعتمدون على الخدمات المصرفية الإلكترونية لتلبية احتياجاتهم المصرفية بسهولة، ولكن في الآونة الأخيرة قد انتشرت عمليات الإحتيال المصرفي الإلكتروني في جميع أنحاء العالم. إن مراقبة المخاطر المرتبطة بهذا الإحتيال وكذلك تقليل تأثيره هي قضية مهمة تواجه المؤسسات المالية حيث أصبحت تقنيات الإحتيال أكثر تقدمًا مع زيادة حدوثها. يعد جهاز الصراف الآلي واحدًا فقط من العديد من أجهزة التحويل الإلكتروني للأموال التي تكون عرضة لهجمات الإحتيال، تتضمن هذه الورقة قنوات احتيالية أخرى مثل الويب والخدمات المصرفية عبر الإنترنت والخدمات المصرفية عبر الهاتف المحمول والشيكات. أجرت هذه الورقة تحليلًا للرصد الإحتيالي عالي الجودة باستخدام مبلغ الخسارة الفعلية للإحتيال في نيجيريا عامي ٢٠١٣ و ٢٠١٤، تم اعتماد تقنية المجموع التراكمي القياسي لمراقبة معدل الإحتيال الإلكتروني لمدة عامين، وكان معدل الإحتيال تحت السيطرة الإحصائية على الرغم من اتجاهه نحو التزايد. وتم تقديم التوصيات على أساس ذلك من أجل الحد من هذا الخطر.

٩) نهج النمذجة للكشف عن الاحتيال ببطاقات الإئتمان في خدمات الدفع الإلكتروني_ ٢٠١٥[٣٧]

ترجع أهمية الدراسة إلى الزيادة في حجم المعاملات الإلكترونية على شبكة الإنترنت في السنوات الأخيرة، ويعود ذلك أساسًا إلى النمو الكبير الذي لوحظ في التجارة الإلكترونية. وهذا السيناريو يجعل عمليات الاحتيال في المعاملات الإلكترونية مسألة ذات أهمية كبيرة. تقترح الدراسة نهجًا شاملًا لمعالجة مشكلة الاحتيال في السوق الناشئة لخدمات الدفع عبر الإنترنت، ذلك عن طريق تقديم نموذجًا لهذه المشكلة، استنادًا إلى تاريخ الكيانات الرئيسية المشاركة في المعاملة لتصنيف ما إذا كانت المعاملة احتيالية أم لا. ومن أجل التحقق من صحة النتائج، تم استخدام بيانات حقيقية مقدمة من شركة كبيرة لخدمات الدفع عبر الإنترنت في أمريكا اللاتينية.

١٠) الاحتيال في التجارة الإلكترونية_ ٢٠١٣[٣٨]

(36) Braimah, O.J & Okonkwo, I.A: 2016, Statistical Monitoring (SM) of Electronic Fraud Occurring in Nigerian Banks, Advances in Multidisciplinary Research Journal _ Vol. 2 No. 3, p. p. 93: 104. https://www.researchgate.net/profile/Joseph-Braimah/publication/328702484_Statistical_Monitoring_SM_of_Electronic_Fraud_Occurring_in_Nigerian_Banks/links/5bdca9e1299bf1124fb56410/Statistical-Monitoring-SM-of-Electronic-Fraud-Occurring-in-Nigerian-Banks.pdf

(37) Gabriel Preti Santiago, Adriano C. M. Pereira, Roberto Hirata, Jr: 2015, A modeling approach for credit card fraud detection in electronic payment services, ACM Digital Library _ Association for Computing Machinery, p. p. 2328: 2331. https://dl.acm.org/doi/abs/10.1145/2695664.2695990

(38) Valentin-Stelian Bădescu: 2013, Fraud in electronic commerce, Perspectives of Business Law Journal _ Issue No: 02 _ Central and eastern European online library, p. p. 8: 20. https://www.ceeol.com/search/article-detail?id=477497

تشهد التجارة الإلكترونية قدرًا كبيرًا من التطور، وبنفس القدر يشهد أيضًا الاحتيال بل أنه أحيانًا يصل إلى مستويات مبهرة. علاوة على ذلك، فإن الاحتيال الحاسوبي لا يبدو أنه يعاني من الركود الاقتصادي العالمي، بل أنه يتطور ويتلاعب أكثر بالمعلومات "جمع ومعالجة وتخزين وتوزيع وما إلى ذلك". ولضمان أمن المعلومات؛ يجب أن يتضمن العنصر المعلوماتي تدابير خاصة بشكل متزايد وبشكل أوسع وأكثر تعقيدًا، لكي يتناسب مع التقدم التكنولوچي لعلوم الكمبيوتر وعولمة المجتمع البشري.

١١) منهجية الكشف عن الإحتيال في المعاملات الإلكترونية_ ٢٠١٢[٣٩]

نظرًا للشعبية المتزايدة للويب، فهناك عددًا متزايدًا من الأشخاص الذين يقومون بمعاملات تجارية إلكترونية. جذبت هذه الشعبية انتباه المجرمين، مما أدى إلى زيادة عدد حالات الإحتيال في الويب بخسائر مالية تصل إلى مليارات الدولارات سنويًا. يقترح هذا البحث منهجية تستند إلى عملية اكتشاف المعرفة، للكشف عن الاحتيال في أنظمة الدفع عبر الإنترنت. من أجل تقييم هذه المنهجية، تم تعريف مفهوم الكفاءة الاقتصادية وتطبيقها على مجموعة بيانات فعلية لأحد أكبر أنظمة الدفع الإلكتروني في أمريكا اللاتينية. أظهرت النتائج أداءً جيدًا جدًا لتلك المنهجية، حيث أنها توفر مكاسب تصل إلى ٤٦.٥٪ مقارنة بالإستراتيجية المُستخدَمة حاليًا.

❖ محور العصر الرقمي

١) إشكالية الهوية العربية الإسلامية في العصر الرقمي_ ٢٠٢٤[٤٠]

تهدف الدراسة إلى بحث واقع العصر الرقمي اليوم وتأثيره على تشكيل الهوية العربية الإسلامية، اعتمدت على المنهج التحليلي والمنهج التفكيكي. توصلت إلى أن قضية الهوية بدأت تأخذ منحنيًا آخر مع ظهور الهويات المتعددة للذات العربية، حيث يتزايد الصراع بين هوية رقمية تسيطر عليها الإغتراب والحداثة، وبين هوية الذات المشبعة بالأصالة والثراث. خلصت إلى أنه بالرغم من هذا التغيير الرقمي، إلا أن الهوية العربية يمكنها استئناف السير مع ركب الحضارة الإنسانية.

٢) أخلاقيات التواصل في العصر الرقمي وانعكاسها على تواصل الجمهور_ ٢٠٢٣[٤١]

(39) José Felipe Júnior, Adriano Pereira, Wagner Meira Júnior, Adriano Veloso: 2012, Methodology for fraud detection in electronic transactions, ACM Digital Library _ Association for Computing Machinery, p. p. 289: 292. https://doi.org/10.1145/2382636.2382697

(٤٠) تهاني الخطيب: ٢٠٢٤، إشكالية الهوية العربية الإسلامية في العصر الرقمي، دراسات العلوم الإنسانية والإجتماعية_ مجلد٥١ عدد٤_ جامعة الأردن، ص ص١٧٢: ١٨٩. https://dsr.ju.edu.jo/djournals/index.php/Hum/article/view/566/1807

تتلخص أهمية الدراسة في أن أخلاقيات التواصل الاجتماعي في البيئة الاتصالية الجديدة تُعد من الموضوعات المهمة جدًا، خاصة عندما رافق هذا العصر الرقمي العديد من المشكلات أثرت بشكل كبير على عملية تواصل الجمهور. استخدم البحث المنهج الوصفي واستمارة الاستبيان. توصل البحث إلى عدم حفاظ أغلب الأفراد على السلوكيات والأعراف عندما يستخدمون مواقع التواصل الاجتماعي، كما أكد المستخدمين على رغبتهم في إدخال نظام يحكم سلبيات وإيجابيات العالم الرقمي.

٣) الثقافة الرقمية للأبناء بين الرفاهية والحتمية في العصر الرقمي "رؤية تربوية"_ ٢٠٢٢[٤٢]

ترجع أهمية الدراسة إلى أن المهارات الرقمية مطلب أساسي في العصر الحالي، حيث يواجه الأبناء مشكلات عديدة عند التعامل مع الشبكة الدولية للمعلومات، تلك المشكلات منها ما يتصل بالجانب الأمني واختراق البيانات، فأصبح من الضروري أن توجد لديهم الثقافة الرقمية، حتى يستطيعوا التعامل مع الإنترنت بشكل آمن والتواصل الرقمي بشكل يحافظ على الخصوصية.

٤) الثقافة والمجتمع في العصر الرقمي_ ٢٠٢١[٤٣]

هدفت الدراسة إلى تفسير تداعيات العصر الرقمي، حيث استندت إلى فكرة أن جوهر الثورة الرقمية يتجلى في التغيرات الثقافية التي تحدث في المجتمع. تم التوصل إلى أن تحولات العصر الرقمي تتلخص في: طمس التمييز بين الواقعية في المجتمع التقليدي والافتراضية في المجتمع الرقمي، التحول من ندرة المعلومات إلى وفرتها. اقترحت الدراسة إيلاء مزيد من الاهتمام للدراسات الثقافية كمحاولة لفهم المجتمع الرقمي.

٥) نهج جديد للإعلان في العصر الرقمي_ ٢٠٢٠[٤٤]

تتمثل أهمية الدراسة في أن الإعلان قد انتشر في ظل تقنيات العصر الرقمي، فتقوم المنظمات بالتسويق عن طريق كسب عقل وعاطفة أفراد المجتمع لشراء منتجاتها عن طريق استخدام وسائل التواصل

---

(٤١) منى تركي شمخي: ٢٠٢٣، أخلاقيات التواصل في العصر الرقمي وانعكاسها على تواصل الجمهور، مجلة آداب المستنصرية_ عدد١٠٤، ص ص٦٨٩: ٧١٦. https://amm.uomustansiriyah.edu.iq/index.php/mustansiriyah/article/download/1123/960

(٤٢) محمود هلال عبدالباسط عبدالقادر: ٢٠٢٢، الثقافة الرقمية للأبناء بين الرفاهية والحتمية في العصر الرقمي "رؤية تربوية"، المجلة التربوية_ كلية التربية جامعة سوهاج_ عدد٩٥ ج١، ص ص١: ١١. 10.21608/edusohag.2022.214740

(43) Ilya Levin, Dan Mamlok: 2021, Culture and Society in the Digital Age, MDPI Journals _ Volume 12 Issue 2. https://www.mdpi.com/2078-2489/12/2/68

(٤٤) إلهام عبدالرحمن إبراهيم شحاته: ٢٠٢٠، نهج جديد للإعلان في العصر الرقمي، مجلة العمارة والفنون والعلوم الإنسانية_ الجمعية العربية للحضارة والفنون الإسلامية_ مجلد٥ عدد٢٠، ص ص ١٦٣: ١٧٨. 10.21608/mjaf.2019.13613.1213

الاجتماعي. وقد يحدث أخبار عاجلة ويتم تداولها، فتبدأ الشركات بإستغلال تلك الأخبار في صياغة فكرة إعلانية، وهو ما يسمى بـ "اصطياد الأخبار Newsjacking". استخدم البحث المنهج الوصفي والتحليلي لمجموعة من المنظمات التي استخدمت اصطياد الأخبار من أجل التسويق الرقمي محليًا وعالميًا. توصل البحث إلى أن استخدام أساليب اصطياد الأخبار تسمح بالتحكم في بناء الرسالة الإعلانية الفاعلة.

تعقيب على الدراسات السابقة

من خلال مراجعة الدراسات السابقة التي تناولت موضوع النصب الإلكتروني؛ اتضح للباحثة أن الدراسات الأجنبية ترجع إلى عام ٢٠١٢م تقريبًا ومستمرة حتى الآن، في حين أن الدراسات العربية بدأت في دراسة ظاهرة النصب الإلكتروني منذ سنوات قليلة فقط. مما قد يوحي إلى أن ظاهرة النصب الإلكتروني ظاهرة قديمة في المجتمعات الأجنبية ومازالت مستمرة، بينما هي ظاهرة حديثة في المجتمعات العربية. ربما يعود ذلك إلى الفجوة الرقمية بين المجتمعات الأجنبية والعربية في استخدام التكنولوچيا ومن ثَم ظهور التسوق الإلكتروني والتجارة الإلكترونية، الذي كان من أبرز نتائجة السلبية ظاهرة النصب الإلكتروني. وقد يبرز ذلك أيضًا مدى أهمية التعرف على أبعاد تلك الظاهرة، ذلك لأنه لم تتم السيطرة الكاملة على عدم حدوثها حتى الآن.

استفادت الدراسة الحالية من الدراسات السابقة في: اختيار نظرية مثلث الاحتيال كنظرية تناسب موضوع الدراسة حيث أنها تنطبق أيضًا مع الجزء الميداني.

تتفق الدراسة الحالية مع الدراسات السابقة في: محاولة السيطرة على تفشي حالات النصب الإلكتروني والتنبوء به من أجل منعه من الحدوث أو إيقافه بأقل الخسائر الممكنة.

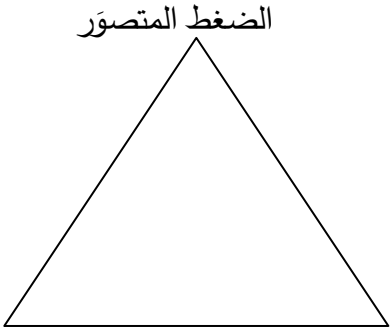
سابعًا: الإطار المنهجي

١) نوع الدراسة ومنهجها

(نوع الدراسة) وصفية تحليلية حيث قامت الباحثة بعرض الوصف الواقعي لكيفية حدوث بعض جرائم النصب الإلكتروني، وحاولت تحليل أحداث جرائم النصب واستنتاج بعض الإجراءات للأمان من الهجمات السيبرانية الهادفة للنصب الإلكتروني. (منهج الدراسة) منهج دراسة الحالة، حيث أنه الأنسب في الحصول على معلومات دقيقة عن الحالات.

٢) نظرية مثلث الاحتيال The fraud triangle theory

تُعتبر النظريات جزءًا أساسيًا من الإطار المُستخدَم لتنظيم ظواهر محددة في العلوم الاجتماعية، حيث توفر نقطة اتجاه للتقييم في منطقة محددة، وبذلك فإن النظرية دائمًا توجه إطار البحث حيث أنها تحدد المتغيرات التي سيتم قياسها. واستنادًا إلى ذلك فإن نظرية مثلث الاحتيال توفر نظرة ثاقبة حول ظاهرة الاحتيال والنصب المالي، حيث افترض كريسي Cressey عام (١٩٧١) أنه من المرجح تفسير حدوث النصب بالنظر إلى ثلاثة من العوامل تمثل شكل مثلث، تلك العوامل عبارة عن (الضغط، الفرصة، التبرير)؛ يشير الضغط إلى الاحتياجات أو الرغبات التي يحتاج النصاب تلبيتها ويمكن وصفها بأنها إما ضغوط مالية أو رذائل، أما الفرصة فالمقصود بها وجود فرصة يستغلها النصاب لإرتكاب النصب وفرصة لإخفاءه لكي يتجنب التعرض للعقاب، والعنصر الثالث لمثلث الاحتيال يتمثل في التبرير أي مبررات يضعها النصاب لنفسه لكي يبرر ويفسر ارتكابه لعملية النصب(٤٥).



- توظيف نظرية مثلث الاحتيال في خدمة الدراسة الحالية

يُلاحظ أن النصب موجود منذ قديم الزمان، بل ويطور النصابون من أنفسهم ليواكبوا مجتمعهم، حتى ظهر لنا الآن النصب الإلكتروني.

فعند دراسة نظرية مثلث الاحتيال يظهر عنصر الضغط على رأس المثلث مما يوحي أنه المتغير الأساسي، في حين يظهر عنصري الفرصة والتبرير في قاعدة المثلث مما يوحي بأنهما متغيرين تابعين، وبالإستناد إلى مسلمات تلك النظرية يمكن توظيفها كما يلي:

(45) Ibanichuka E.A.L, Oko I. A.:2019, Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria, International Journal of Advanced Academic Research | Management Practice _ Vol. 5 _ Issue 4, p. 19. https://www.ijaar.org/articles/Volume5-Number4/Management-Practice/ijaar-mp-v5n4-apr19-p2.pdf

(الضغط): قد انتشرت ظاهرة النصب الإلكتروني في الآونة الآخيرة بكثرة، ربما يعود ذلك إلى ضغط رئيسي على النصابون وهو الزيادة الباهظة في الأسعار في السنوات الأخيرة.

(الفرصة): قد وفرت التكنولوچيا المتسارعة في التطور فرصًا عديدة للنصابون فاستطاعوا التواصل مع الكثير من الضحايا، بل أن النصابون يبدعون في خداع هؤلاء الضحايا في وقت قياسي جدًا خصوصًا عن طريق شبكات التواصل الاجتماعي. وللأسف أيضًا فإن استخدام جميع الأفراد غالبًا للأجهزة الإلكترونية الحديثة والإنترنت، قد وهب النصابون فرصة عظيمة للإختفاء وتدبير وتنفيذ جرائمهم خلف ستار التكنولوچيا المتسارعة هي الآخرى في التطور المستمر.

(التبرير): إن ظهور فئة من الأفراد الأغنياء بدرجة باهظة قد أوجد فجوة بين الطبقات، حيث وجود طبقة تستطيع شراء كل شيء وبأعلى الأسعار في مقابل طبقة أخرى تعاني من القدرة على توفير متطلباتها الأساسية في ظل الإرتفاع المتزايد بل والمستمر يوميًا في بعض الأوقات، مما أوجد طبقة تريد أن تحصل على المال بدون تعب وبكل سهولة، وتبرر لنفسها أن من حقها الأساسي في الحياة أن تكون مِثل أولئك الذين لديهم درجة عالية من الرفاهية. وتنوه الباحثة أن الضغوط المتوالية بسبب ارتفاع الأسعار ليس مبرر بأن تسول بعض الأنفس لأصحابها بإرتكاب جرائم النصب الإلكتروني.

٣) أداة الدراسة

استخدمت الدراسة دليل دراسة الحالة، حيث تألف من (٤) أسئلة مفتوحة؛ البيانات الأساسية للجاني، وللمجني عليه، وكيفية حدوث جريمة النصب الإلكتروني، وتعليق شخصي للمجني عليه بعد خوض تلك العملية الموجهة للنصب عليه إلكترونيًا. وتمت المقابلة ومناقشة الإجابات والاستفسار عن التفاصيل عبر تطبيق .Whats App.

٤) مجالات البحث

- المجال الجغرافي: تمت الإجراءات الميدانية للدراسة في بعض محافظات مصر، حسبما أُتيح للباحثة، أي لم يتم التحديد مسبقًا:

  الجُناة: (دمياط ،الإسكندرية، أماكن غير معروفة).

  الضحايا: (دمياط، بورسعيد، شربين، المطرية دقهلية).

- المجال الزمني: (ست شهور تقريبًا) بداية من شهر سبتمبر ٢٠٢٣م، حتى مارس ٢٠٢٤م.

- المجال البشري: تم تحديد نوع عينة البحث بأنها (عمدية) من الأشخاص الذين تعرضوا للنصب الإلكتروني، عددهم (٢٠) حالة.

٥) الحالات

حالة (١)

أولًا: البيانات الأساسية: (الجاني: شخص على انستجرام) (المجني عليها: ٢٥ سنة_ عزباء_ الحالة الاقتصادية متوسطة)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: اتعرفنا بشكل شخصي لدرجة إنه عرفني على عائلته، قالي إنهم من الخليج وعندهم منزل هناك ومنزل آخر في المغرب، تبادلنا الصور ومحادثات فيديو بين عائلتي وعائلته، وبعتلي صورة بطاقته وباسبوره، والدته قالتلي إنها مرتاحة لي وأحبتني، وصرح والده بحب ابنه لي وأنه سعيد بمعرفتي. بعد شهرين الشاب قالي إنه يريد الزواج مني، وكان بيحكي عن مدى نجاح زواج والديه. كان بيقولي إنه هيشتري منزل لعائلتي، أنا لست بحاجة للمال لكنه بعد رفض شديد مني أرسل لي أيفون آخِر إصدار وكان بيرسل لي مبلغ مالي كل شهر وملابس أيضًا، كان بيرسلهم بإسمه ورقم بطاقته مما جعلنا مطمئنين له جدًا. في يوم قالي إنه سوف يزور بلدي لكي يقابل عائلتي ويأخذ منهم ميعاد لكي تأتي عائلته ويخطبوني ثم عقد القران، وأخبرني عن مكان لكي يقوم والدي بالسؤال عنه وعن عائلته فيه، وبالفعل ذهب والدي وسأل عليه وأكد حارس المكان على هويته وهوية عائلته، وكنت على تواصل معه في كل تحركاته عن طريق الفيديو أثناء شرائه لكل شيء يخص منزل الزوجية. أنا وأختي وزوج أختي استقبلناه في المطار ووصلناه إلى الأوتيل الذي قام بالحجز فيه من بلده ولم يوافق أن نقوم بالحجز له نهائيًا، ثم تعرف علي باقي عائلتي واتفقنا على كل شيء وسافر بلده واتطمنت عليه فيديو لما وصل، وحددنا موعد الخطبة بعد العيد بعد ٢٥ يوم، وقالي هييجي معاه عائلته عددهم (٨) وأرسل لي أموال لضيافتهم. وفي يوم أتى الشاب وجلب معه هدايا وبرفانات وملابس، وقالي أقوم بفتح الملابس بمفردي لأنها ملابس خاصة، اندهشت بالملابس كثيرًا وظل في بلدي ٤ أيام أول يوم كان بالأوتيل والثاني جاء لزيارتنا والثالث اتعشينا في مطعم أنا وهو وأختي وزوج أختي واليوم الرابع والدي عزمه على العشاء، وبعد ذلك ذهب إلى المطار ليسافر بلده. في خلال الـ٢٥ يوم اللي اتفقنا عليهم، دخل لي شاب من رقم مجهول على الواتساب وتعرف عليا وقالي إنه صديق عريسي، استغربت وتوترت جدًا إنه إزاي عريسي يدي رقمي لشاب آخر، ولما سألت عريسي رد قالي إنه معرَفش رقمي لحد، ونهى الحوار لكن أنا

كنت لسه حاسة بعلامات استفهام وخوف لأني أحببت عريسي بشكل مبالغ فيه، وكنت بسمع كلامه في كل شيء واديته الأمان لدرجة إنه طلب مني أن أتصور بالملابس اللي جبهالي وابعت له الصور وفيديوهات وأنا وافقت. جاء أهله في الموعد المحدد واتعرفوا على أهلي وتمت الخطبة، كان بيضغط عليا باستمرار بإلتقاط صور ليا وفيديوهات وإرسالها له حتى بدأت أخاف من طلباته ونفسيتي بدأت في الدمار عندما هددني إني لو مبعتلوش الصور والفيديوهات هيطلب أموال مني، وفعلًا كنت ببيع أشياء من منزل والدي وأرسل له أموال، حتى طلبت منه معرفة كل شيء ورائه ووراء مطالبة، صرَح لي عن هويته دون كذب هذه المرة، قالي إنه عضو في خلية خاصة بهذه الأعمال الفاحشة التي تؤدي لدمار الفتيات وتحول حياتهم نحو الجحيم، فبدأ التعب يظهر عليا، امتنعت عن الطعام وانعزلت عن البشر ورفضت إكمال دراستي وحاولت الانتحار لكن المحاولة لم تنجح، هنا تدخل أهلي وسألوني عن تفاصيل ما يحدث وحكيت لهم، والدتي توجهت لجمعية حقوق الإنسان وهنا تدخلت الشرطة الإلكترونية بعد محاولات شاقة لقبول ملف القضية، وتمت التحريات عنه وتوصلوا أن الاسم اللي أرسل منه الأموال والبطاقة مزورين وصاحب البطاقة الحقيقي متوفي من ٥ سنين، ولما تابعوا مكالماته عرفوا إنه لما كان بيعدي من المطار كان فيه حد تبعه بيختمله الباسبور وبيعدي عادي. استمر في تهديدي ووصف أشياء معينه في منزلنا لبيعها لإرسال الفلوس له حتى إن والدي باع سيارته، وإذا لم أقوم ببيع شيء فأقوم بعمل الفيديوهات، مكونتش قولتله إني عرْفت أهلي بالحقيقة فكان بيقولي أقولهم إني لا أرغب بالزواج منه. عندما هددته إني هبلغ أهله عن كل اللي بيعمله معايا، قالي إنهم مش أهله أصلًا، وهم ناس بيخدموه عشان اللعبة تتم، وقالي إن أول صوره ليا بعتهاله كان أرسلها للخلية ووافقوا عليا وقالوا إن فيا المواصفات المطلوبة، بدأ يرسل لي فيديوهات لكي أقوم بتقليدها، الشرطة قالولي أسايره في كلامه وأنفذه، الجاني قالي إن اللي بيتفرجوا على فيديوهاتي طالبيني شخصيًا، رفضت، قالي إنه هيزورلي بطاقة باسم مستعار وملف دراسي على أساس إني هسافر أدرس هناك، رتبت كل شيء مع المخابرات، والجاني قالي إن الخلية ١٤ فرد منهم من دِوَل أخرى حيث أنهم اخترقوا حساب لشخص غني في إحدى البنوك وسرقوه عن طريق واحدة بتشتغل في البنك، روحت في الميعاد اللي حدده الجاني، وكان قايلي إنهم هيصوروا فيديوهات لي دون رفض واعمل اللي يطلبوه، لكن الشرطة وصلت كما تم الاتفاق بيننا وتم القبض عليهم جميعًا في البلد اللي سافرتله فيها واتضح إنه من طبقة متوسطة وعنده ٢٨ سنة.

حالة (٢)

أولًا: البيانات الأساسية: (الجانية: م_ ٢٣ سنة_ إسكندرية_ تعليم عالي_ مخطوبة_ أفراد الأسرة "٥") (المجني عليها: ن_ ٢٠ سنة_ دمياط_ تعليم عالي_ عزباء_ أفراد الأسرة "٤")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: اتعرفت على النصابة على Facebook عن طريق إعلان كانت كاتباه عن فرص عمل في شركة بمرتب يتعدى ٣٠٠٠ آلاف إسبوعيًا، وعندما علقت لها على هذا الإعلان فردت عليا خاص وحددت موعد معايا لمقابلة لفهم تفاصيل الشغل. في المقابلة قالتلي إن العمل عبارة عن: تسويق للملابس، أو إني أدَخل الشركة عملاء جُدد وليا مبلغ مالي لكل عضو جديد ادخله المجال، أو اشتري توكيلات لكي يكون ليا امتيازات مثل تخفيض على الأدوية أو فلوس كاش أو خصم عند شراء الملابس أو حتى أخذ ملابس ببلاش لكن كل هذا على حسب سعر كل توكيل سواء بـ٥٠٠٠ جنيه أو بـ ١٥٠٠٠ جنيه أو بـ ٢٥٠٠٠ جنيه. فأنا عملت فحوصات وسألت عن الشركة ومقرها وبياناتها، فوجدت أنها تقوم بالتهرب الضريبي منذ ٣سنوات وحاصلة على عدد كبير من القروض لم يتم سدادها، ومع مرور الوقت تم غلق تلك الشركة.

حالة (٣)

أولًا: البيانات الأساسية: (الجاني: بنك توسونجوك) (المجني عليه: م.ن_ ٣٨ سنة_ بكالوريوس تجارة جامعة طنطا_ محل الإقامة شربين دقهلية_ مستوى اقتصادي متوسط_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كان فيه إعلانات لبنك افتراضي على Facebook بيتم شراء أسهم فيه عن طريق تحويل المبالغ على حساب البنك، بمعنى أن البنك له حساب حقيقي بيتم إيداع الأرصده عليه، ومكان المدراء في مدينة إسطنبول بتركيا لكن التداول إلكتروني ولا يوجد مبنى للبنك، كان بيسمح بشراء الأبقار والماعز والخراف واللحوم والبيض لكن بشكل افتراضي بحيث يكون لكل مساهم ما يشبه الحظيرة الافتراضية، يستطيع من خلالها جمع وإعادة بيع ما يمتلكه. البنك كان يمنح أرباحًا عالية جدًا "خيالية" كل عام فحاز على شعبية هائلة بعد ٦ أشهر فقط من ظهوره، لكن كان بيفترض قيودًا زمنية على إمكانية إعادة البيع يعتبرها العمر الافتراضي للمادة التي يتم شرائها بحيث لا يمكن بيع الخروف قبل مرور عام والماعز قبل مرور سنتين واللحوم بعد ٦ أشهر وهكذا، في فترته الأولى كان بيدي عائد حقيقي، لكن بعد مرور سنة ضعفت قدرته على دفع الأموال للمستثمرين الذين يريدون بيع ممتلكاتهم

الافتراضية، مما جعل المزيد يريدون التخلي عن ممتلكاتهم. قام البنك الافتراضي بتحويل رصيده من بنك إلى آخر، وفجأة اختفى.

حالة (٤)

أولًا: البيانات الأساسية: (الجاني: شخص على Facebook) (المجني عليها: ١٧ سنة_ الفرقة الأولى بالجامعة_ عزباء_ محل الإقامة المطرية دقهلية_ مستوى اجتماعي اقتصادي متوسط_ تعليم الأب والأم متوسط)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كانت الفتاه تتسوق إلكترونيًا لشراء موبايل iPhone ثمنه المعروف: ١٥ ألف جنيه. فوجدت إعلان على Group في Facebook في نهاية عام ٢٠٢٢ أن سعر الموبايل هو ٧٠٠٠ آلاف جنيه فقط. قالت الفتاة أن ما جعلها تصدق هذا الإعلان هي عروض نهاية العام المشهورة، والـ Friday أو ما يطلق عليها الجمعة البيضاء أو السوداء، بالإضافة إلى زيادة الجمارك وتعويم الجنية وتنافس المواقع على بقاء السعر القديم أو أقل سعر، بالإضافة إلى أن هذا الـ Group لديه عدد من الأعضاء ما يكفيه لإثبات صدقه. انضمت الفتاه لهذا الـ Group وسرعان ما أُرسِل إليها Link انضمام لبرنامج Telegram كي يتم الرد سريعًا، وتم إضافتها في Telegram Group يتم إرسال عليه تعليقات إيجابية عن مدى الإلتزام بالتسليم قبل الموعد المحدد وكم هو جيد في التعامل، فأخبرته بأنها تريد الهاتف بالسعر المعروض، فسألها إذا كانت مشتركة في مواقع شراء OnLine وأنه يريد نصف المبلغ قبل أن يُفَعِل لها حساب على إحدى مواقع الشراء وطلب منها بيانات شخصية، وسألها إذا كان لديها بطاقة بنكية ولحسن حظها أنها لا تمتلك، فأرسل لها رقم موبايل لتحويل المبلغ عليه، وتم إرسال إليها أنه تم تفعيل حساب لها، وعلى حد قولها أنها بذلك تأكدت من صدق نيته، وأخبرها أنه في غضون خمس أيام سيصل الهاتف لكن بعد أن تكون أرسلت باقي المبلغ. دفعت الفتاه كل المبلغ المطلوب بدون علم أحد، وبعد مرور ٣ أيام اتصلت بصديقتها لتخبرها بأنها عاجزة عن التصرف، لأنه تم حظرها وتجاهلها وعدم الرد عليها، وبعد نقاش اتفقن على الانتظار حتى تمر الفترة الباقية، لكن بعدها تم إبعادها عن المجموعات والصفحات والأرقام وكل ما يتعلق بهم، وهكذا وقعت الفتاه في الفخ.

حالة (٥)

أولًا: البيانات الأساسية: (الجاني: شخص على Facebook) (المجني عليها: ١٨ سنة_ ثانوية عامة)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كنت عاملة صفحة على Facebook من ٥ سنين، ووصل المتابعين فيها ١٠ آلاف. في يوم وصلني Link لشغل تسويق من صفحة أكبر من صفحتي عليها ٢٠ ألف متابع، أول ما دخلت على الـ Link صفحتي اتهكرت (اتعمل تسجيل خروج من اللابتوب والموبايل، والباسوورد والإيميل اتغيروا، وكل ده في ثانية) بعد ساعة الهاكر نزل صورة مستشفى قدام غرفة العمليات على Story صفحتي، وكتب إن ماما بتموت وعمليتها واقفة على مبلغ معين والحالة بتسوء مع الوقت وإن عمري ما كنت هطلب فلوس من حد لولا الزنقة، وطبعًا الصفحة عشان عدد متابعيها ضخم ماتقفلتش بالتبليغ عنها، طبعا حاولت انزل إن الصفحة اتسرقت لكن أكيد مقدرتش أوصل لكل المتابعين، للأسف أنا تعبت في صفحتي دي جدًا لكن ضاعت، ده غير تعب الأعصاب اللي حصلي ليلة امتحاني. كمان عايزة أقول إني عملت صفحة جديدة ونزلت بوست إن صفحتي القديمة اتهكرت، وللأسف دخل ليا ناس كتير جدًا قالولي إنهم حولوا مبالغ كبيرة فعلا على فودافون كاش للصفحة القديمة.

حالة (٦)

أولًا: البيانات الأساسية: (الجاني: هاكر على Facebook) (المجني عليه: ٢٠ سنة_ شربين_ طالب جامعي_ أعزب_ أفراد الأسرة "٤")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: صديقي بعتلي رسالة من الأكونت بتاعه إن أخته تعبانه ومحتاج (١٠ آلاف جنيه) فبعتلوا المبلغ على رقم فودافون كاش اللي بعتهولي، بعد كده أكونت صديقي اتقفل ورقم فودافون كاش اتقفل، الأكونت كانت متهكر والهاكر قفل الأكونت بعد عملية النصب، عملت محضر في النيابة لكن لسه لم يتوصلوا للنصاب.

حالة (٧)

أولًا: البيانات الأساسية: (الجاني: هاكر على الموبايل) (المجني عليها: س_ ٢٢ سنة_ دمياط_ دبلوم زراعة_ متزوجة_ أفراد الأسرة "٤")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: جيت ليا رسالة من رقم موبايل على موبايلي: تم إيقاف حسابك البنكي الرجاء الاتصال لتجديد بياناتك، فأنا رنيت على الرقم، فرد شخص قالي نازل لحضرتك تحديثات شهر ٧، وسألني ليكي أي حسابات تانية؟ قولتله هو الحساب ده فقط، بعدين سألني عن المبلغ الموجود في الفيزا، قلتله ٣٥٠٠٠ ألف جنيه، قالي فيه موجود أرقام على ضهر الفيزا مليهالي، فمليتهالوا، قالي هيجيلك رسايل كل رسالة توصلك مليهالي وبعدين امسحيها، مليته كل الأرقام. بعدها بإسبوع روحت

اسحب الفلوس ملقتش فلوس في الفيزا وكانت فاضية، روحنا المنصورة نبلغ، وللأسف قالولي مش هتقدري توصلي للنصاب.

حالة (٨)

أولًا: البيانات الأساسية: (المجني عليها: ٢٥ سنة_ تعليم متوسط_ ربة منزل_ متزوجة من شخص غير مُتَعلِم يعمل عامل حر_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: وصلت رسالة إلى الضحية على Facebook من صديقتها، تطلب منها تجمع تبرعات لأن زوجها تعبان جدًا ومحتاج عملية في القلب وقالت إنه مُعرَض للخطر وممكن يموت في أي لحظة لإنه مريض سكر ومحتاج شريط السكر لإنه خلص والعملية هتتكلف مبلغ كبير. جمعت الضحية بالفعل مبلغ (١٣٠٠ جنية) وحولتلهم على رقم صحبتها (كمان جابت ليها الأدوية). بعد فترة (الضحية شافت إن صحبتها دي منزلة نفس الكلام في جروبات وكمان منزلة صور الإشاعات الطبية، ولما سألت اكتشفت إن صحبتها دي بتعمل كدة علطول مع كذا فرد قبل كدة، فبلغت الناس اللي في الجروبات بكدب النصابة دي، لكن لم تستطع رد حقها وحق فلوس الناس حتى الآن).

حالة (٩)

أولًا: البيانات الأساسية: (المجني عليه: ٤٥ سنة_ تعليم عالي_ من دمياط يعمل بالإمارات_ المستوى الاقتصادي متوسط_ متزوج_ أفراد الأسرة "٦")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كنت اعرف شخص سواق على عربية، بدأ مظهره يتحسن وأهل بيته كمان شكلهم بقى أفضل، التغيير ده كان أغلب الناس واخده بالها منه، مكونتش بكلمه لكن هو عارف إني مسافر. بعد فتره لقيته بيتواصل معايا على النت، وقالي إن بقى حالة ميسور وسعيد بسبب إنه بيشغل فلوس لناس في مشاريع وفاتح مكاتب في المينا، وعرَض عليا ادخل معاه بمبلغ مالي، الغربة خليتني افكر إني اسيبه يشغل لي فلوسي ونعيش بالفوايد وانزل اقعد مع عيالي، قالي إن كل ٥٠ ألف جنية عليهم فوايد ١٥٠٠ كل شهر والمبلغ الأصلي زي ماهو وأي حد يقدر يسحب فلوسه في أي وقت لكن يعرفني قبلها بشهرين، فعلًا في الأول فضل يدي الفوايد في مواعيدها بالظبط لحد ما الناس طمعت وزودوا الفلوس بتاعتهم معاه، جمع من الناس ٢ مليون و٨٠٠ ألف، لكن فيه بعض أشخاص طلبوا فلوسهم فهو أدى لأربع أشخاص مبلغ وبعدين قال إنه اتنصب عليه ومفيش معاه فلوس يرجع للناس

حقها. أنا وناس كمان كان معانا شيكات ليه، عملنا محضر ودخل السجن، لكن مخدناش حاجة من فلوسنا، وندمت إني خسرت اللي فضلت سنين اجمعه.

حالة (١٠)

أولًا: البيانات الأساسية: (المجني عليه: م_ ٥٤ سنة_ تعليم متوسط_ الزرقا دمياط_ المستوى الاقتصادي متوسط_ متزوج_ أفراد الأسرة "٤")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كان ليا صديق طفولة لكن مكوناش بنتكلم من فترة كبيرة، فجأة لقيته بيكلمني على النت قالي إنه معاه شغل حلو محل موبيلات ومكسبه كويس، بعتلي صورة المحل كان في حي شعبي الهرم القاهرة فسافرت شوفته على الطبيعة كان فعلًا شغال كويس، هو كان عايز شريك بالنص عشان يجيب موبيلات مستعمله يبيعها، دفعتله ١٢٠ ألف واشترى فعلًا موبيلات، كان بيعملي جرد يومي وآخد الفوايد بنسبة الثلث آخر الشهر معدل ٤ أو ٥ آلاف جنيه في الصيف والشتا مريح شويه، وهو كان بياخد التلثين عشان أجور العمال. حصلي ظروف مفاجأة واحتجت فلوسي في ظرف شهر واتفقنا على كده، جه الشهر لكن قالي والله مش عارف لسه ابيع أو اصفي اصبر عليا شهر كمان، بعد الشهر التاني روحت له المحل لقيت صاحبه بيستلمه فاضي مفيش فيه أي بضاعة ونصب عليا وعلى غيري بنفس الطريقة وسافر ليبيا، قعدت أحاول اتصل بيه مفيش، عرفت بنته متجوزه فين روحت عملت مشكلة عند جوزها وحضْرت ناس كبيرة وجوز بنته دفعلي ٢٠ ألف وقالي مليش دخل بالموضوع ده.

حالة (١١)

أولًا: البيانات الأساسية: (المجني عليه: م_ ٥٠ سنة_ تعليم متوسط_ الزرقا دمياط_ متزوج)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: صديق ليا قريبي شاف على النت إن فيه أرض زراعية ٥٠ فدان في الوادي الجديد، صاحبها عايز يستصلحها، وبيبحث عن ممولين. سألته إنت ضامنه النت ده؟ قالي تعالى نشوف كده الأرض وسافرنا، الأرض مكانتش مزروعة لكن كانت جاهزة للزراعة، صاحبها قال إنه هيزرعها بنجر وفواكهة وحاجات عديدة عشان الأرض خصبة جدًا، قال إنه محتاج مليون جنيه، وبعد خمس سنين كل واحد هيرجعله المبلغ اللي دفعه بالفوايد. جابلنا عقد شراكة إن إحنا بالفلوس وهو بالأرض، وقال إنه من الشهر العقاري، كنا مصدقينه لإنه بدأ يعمل معانا علاقة صداقة وعزومات غدا

وعشاء ومقابلات، وكنا متابعين معاه الأخبار لكن فجأة بعد شهرين اختفى، سافرنا نشوف الأرض اكتشفنا إن الأرض مش بتاعته وكان مأجرها سنة، فِضل فيها شهر وسابها، فضلنا ندور عليه وبلغنا البوليس ولحد الآن مفيش خبر عنه بعد ما كل واحد فينا دفعله ٥٠٠ ألف جنيه.

حالة (١٢)

أولًا: البيانات الأساسية: (المجني عليها: ٢٠ سنة_ طالبة جامعية)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كنت أنا وزميلتي في الدفعة بندور على شغل على النت، زميلتي وجدت واحدة قالتلها ادفعي تأمين ٢٥ جنية عشان تشتغلي معايا، هتنزلي إعلانات لمنتجات على صفحات التواصل الاجتماعي بتاعتك، وهتاخدي آخر الشهر ألفين وخمسمائة جنيه. بالفعل زميلتي استمرت طول الشهر في تنزيل الإعلانات (ولما جه آخر الشهر، النصابة عملت لزميلتي بلوك، ومااديتهاش فلوس).

حالة (١٣)

أولًا: البيانات الأساسية: (المجني عليها: ع.م_ ٢٠ سنة_ طالبة جامعية_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: طلبت الضحية أوردر من جروب بالفيسبوك، فصاحبة الجروب طلبت منها التفاصيل ونصف ثمن الأوردر لضمان الجدية، بالفعل دفعت الضحية "٦٠٠ جنية" لكن النصابة ادعت أن المبلغ لم يصلها (وقالت للضحية إنتي نصابة) الضحية قالت للنصابة لو مرجعتيش الفلوس، هنشر اسمك وصورتك ورقم موبايلك في جروب عام، فالنصابة شتمتها وعملت لها بلوكات.

حالة (١٤)

أولًا: البيانات الأساسية: (الجاني: دمياط) (المجني عليها: ٦٠ سنة_ بورسعيد_ دبلوم تجارة_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: الجاني كان بيعرض صور لغرف نوم على Facbook الضحية اتفقت معه على عمل غرفة لإبنها بـ٣٠ ألف جنيه. طلب ألف جنيه عربون على فودافون كاش فأرسلت له المبلغ، بعدين طلب مبلغ عشر آلاف عشان يخلص الغرفة فأرسلت له المبلغ، عندما تأخر

عليها في تسليم الغرفة كلمته، قالها تبعت كمان ٧ آلاف جنيه فحولتهم له. بعد ذلك سألته على الشغل قالها لسه، كلمت ناس من بلده، فقالها مالكيش حاجة عندي دلوقتي ولما ابقى اخلص ابقى اكلمك، ونصب عليهم وهي الآن عملت محضر لكن دون جدوى حتى الآن.

حالة (١٥)

أولًا: البيانات الأساسية: (الجاني:شخص على إحدى مواقع التواصل الاجتماعي) (المجني عليها: ثانوية عامة_ عزباء_ ١٨ سنة_ محل الإقامة دمياط_ المستوى الاجتماعي متوسط_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: أخت زميلتي اقتنعت إن فيه شخص بيعرف يعَدِل درجات الثانوية العامة، عن طريق اختراق سيرفرات وزارة التربية والتعليم. قالها ابعتيلي رقم جلوسك، وعايزة تعملي إيه علشان أقولك على السعر، قالتله عايزة ارفع الدرجات لـ (٩٠%) عارفة إن المعدل كبير لكن هو ده اللي كنت استحقه، قالها حوليلي (٩٨٠٠ جنيه) قالتله التعديل امته، قالها النهارده، وبعتلها اسكرينات لنتايج معدِلها قبل كده، قالتله أنا عايزاها تتغير على صفحة النتائج مش تبقى اسكرين، قالها اطمني أول لما تحولي المبلغ هتلاقي نتيجتك على الموقع ٩٠% وآخر ميعاد للتحويل هيكون الساعة ١٠ لإن بعدك دُفع تانية. حولت له المبلغ، وبعدها بتكلمه بيشوف الرسايل ومش بيرد وبعدين عملها بلوك، أختها دخلتله من رقمها قالتله إحنا عرفنا إنك بترفع الدرجات فعاوزة ارفع درجاتي وهدفعلك اللي إنت عايزه، سألوه ممكن يكلموه فون قالهم ممنوع، وطلب منها رقم الجلوس فبعتوله رقم مزيف، وسألها عايزة ترفعي أد إيه، قالتله ٨٠% طلب منها مبلغ ٦٠٠٠جنيه، وسألته هنتقابل فين عشان أديك المبلغ فماوافقش، وقالها الدفع اتصالات كاش، سألته إنت منين معتش رد نهائي، وطبعًا بينزل استوريهات لنتائج طلاب لناس تانية بإنه زودها، ورقمه كان بعدها مغلق.

حالة (١٦)

أولًا: البيانات الأساسية: (الجاني:شخص على .Whats App) (المجني عليها: م_ ٢٢ سنة_ تعليم عالي_ عزباء_ دمياط_ أفراد الأسرة "٦")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: شخص كلمني من رقم دولي باللغة الإنجليزية، وقالي عندي ليكي شغل إنك تعملي إعجاب للمنتجات، وفي المقابل بتاخدي ٤٠ جنيه، فوافقت، وبعت فعلًا لي ٤٠ جنيه على فودافون كاش، بعد كده دخلني على جروب تليجرام. بنت من اللي معاه قالتلي ليكي ٢٤

مهمة لو خلصتيهم بتاخدي مكافئتك؛ قالتلي ابعتي ٣٠٠ جنيه على الرقم وهتتردلك ٤٠٠ وبعتتني لحد اكبر منها (ت) وقالي اعملي نفس الخطوات اللي في الأول وبعدها قالي ابعتي ١٠٠٠ جنيه وبعدها قالي التاجر عايز ٥٠٠٠ جنيه وبعدها قالي التاجر عايز مهمة أخيرة ١٥ ألف جنيه، ولما قلتله مش معايا المبلغ قالي لازم تتصرفي عشان اللي دفعتيه ميضيعش. جروب التليجرام كان عليه Screenshot لناس حولت ولمكاسبهم، وكل لما اكلم حد من الناس دي يعملولي بلوك، وبكده فهمت إني اتنصب عليا وكله كان فيك.

حالة (١٧)

أولًا: البيانات الأساسية: (الجاني: أ.م_ شخص على شبكات التواصل الاجتماعي) (المجني عليها: ن.ج_ ٣٥ سنة_ دبلوم تجارة_ متزوجة "أم"_ دمياط_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: كان لدى الضحية متجر لبيع الملابس، أرادت أن تروج له على وسائل التواصل الاجتماعي، كانت تمتلك منصة على أحد البرامج الإلكترونية فأرادت أن يرى سلعتها أكبر عدد من الناس، فتواصلت مع الجاني الذي يعمل في تسويق وترويج السلع عن طريق إعلانات ممولة للمنصات المختلفة بمقابل مادي، كان يشترط أن يحصل على المقابل المادي للإعلان كاملًا قبل أي شيء، الضحية أرسلت له المبلغ، قام الجاني بحظرها ولم تستطع الوصول إليه.

حالة (١٨)

أولًا: البيانات الأساسية: (الجاني:شخص اتصل على الموبايل) (المجني عليها: أ.إ_ ٣ ثانوي عام_ عزباء_ دمياط الجديدة_ أفراد الأسرة "٥")

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: الجريمة حصلت مع صحبتي وقت الظُهر، رقم الجاني كان متسجل على التروكولر بإسم شخص (فعادي يعني ردت عليه) قالها مساء الخير يافندم حضرتك من الأرقام المميزة وفوزتي معانا بمبلغ مادي (كان كذا ألف) طلب فيزا لتحويل المبلغ عليها، فنهضت بسرعة وأخذت فيزا مامتها اللي كانت نايمة فلم تعرف ما يجري، وأكملت معه الحوار حيث كان يتحدث بطريقة لبقة جدًا وثقة كأنه يعمل في بنك حقيقي، طلب رقم الفيزا وجميع البيانات الموجودة عليها والرقم السري، ثم وصل رسالة من البنك مكتوب فيها الرقم التأكيدي، قالت لمامتها تقولها الرقم لكن كان انجليزي فلم تعرف، فصحبتي قرأته هي للجاني بسرعة، هنا تأتي الصدمة من مامتها إنها جيت لها رسالة تم سحب

ألف جنية، هنا أغلقوا الاتصال بسرعة، ثم وصلت رسالة بسحب ألف ثاني ثم ألف ثالث، وكان سيكمل لولا فضل الله جاء لمامتها اتصال من البنك أن السحب غير منتظم هل هناك مشكلة؟ فأبلغتهم ما يحدث فأغلقوا لها الحساب تمامًا.

حالة (١٩)

أولًا: البيانات الأساسية: (الجاني:شخص على شبكة تواصل اجتماعي) (المجني عليه: مازن)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: طلبت هدوم أون لاين، والبوست بتاعها كان باين الخامة والتصميم حلوة جدًا، بس لما الأوردر وصل كان لا خامة ولا أي حاجة، ولا كان فيه أي مصداقية، لكن اضطريت ادفع الفلوس لإن اللي جايب الأوردر مالوش ذنب إنه يشيل تمنه. من بعدها حرمت اشتري أون لاين.

حالة (٢٠)

أولًا: البيانات الأساسية: (الجاني:شخص على شبكة تواصل اجتماعي غير مشهورة) (المجني عليها: ٢٨ سنة_ تعليم عالي_ عزباء_ الحالة الاقتصادية متوسطة)

ثانيًا: كيفية حدوث جريمة النصب الإلكتروني: حكايتي حصلت على فترتين (فترة من عشر سنين تقريبًا، وفترة من ثلاث شهور) النصب حصل معايا في الفترة الأولى، ومحصلش في الفترة التانية لإني كنت أخدت خبرة. بداية الموضوع إن فيه شخص دخل اتعرف عليا برسايل على الخاص (قالي إنه ضابط طيار، من القاهرة، أكبر مني بفرق سنين بسيط، اسمه يوسف، بيشتغل في مطار الإسماعيلية) يمكن كان من الأسباب الرئيسية اللي خليتني أوافق ابعتله فلوس: إني كنت قلقانه منه بعد ما اتكلم معايا كلام أوفر شوية في الموبايل وقالي إنه عايز نتجوز، ومن ناحية تانية قلت بردوا لما أشوف آخره إيه وهو عايز يوصل لإيه بالظبط. أول مرة يطلب مني فلوس، كان عامل نفسه مصدوم وقالي بنفسه: مش واخده بالك إن نبرة صوتي متغيرة عن العادي عشان يلفت نظري وأصدقه يعني، كان بحجة إني الكوتشي بتاعه اتسرق منه في الفندق وهو مسافر برا مصر، ومكانش عامل حسابه في فلوس ومحرج يطلب من حد، طلب ألفين جنيه عشان هو بيلبس ماركة غالية، بعتله المبلغ على فودافون كاش. المرة التانية اللي طلب فيها فلوس كان بحجة إنه في الإسماعيلية وكان فاكر إنه هيروح بيته لكن فيه شغل إضافي وهيضطر يقعد فترة أكبر ومش عامل حسابه في فلوس، والمرة دي قالي أروح موقف دمياط أسأل عن سواق اسمه

إدريسه هو عارفه، وابعت معاه ست ألاف جنيه، واتابعه من بعيد اتأكد إنه خرج من الموقف عشان النوعية بتاعته دي طماعه وممكن ميسافرش بسرعة ويستنى يحمل ركاب، مع إني دفعتله تمن أجرة العربية ٥٠٠ جنيه، وقالي أقول للسواق إن اللي هيستلم منه المبلغ واحد عسكري بلبس ميري عشان يسافر بسرعة يعني ومش يتأخر. المرات اللي بعد كده اللي كان بيطلب فيها فلوس كان بيطلب احوله كروت شحن موبايل أو فودافون كاش، بحجة إنه مسافر ومش معاه فلوس شحن وعايز يعمل مكالمات دولي مهمة، طبعا كان أيامها لسه مظهرتش مكالمات النت الرخيصة زي دلوقت. نصب عليا في ١١ ألف جنيه تقريبًا، وبعدين لما اتكررت مرات الهروب إنه ياخد خطوة إيجابية ونتقابل عشان جواز رسمي زي ما قالي، أنا بعدت ومعوتش برد عليه. من سنتين ونص كده في حساب بعتلي صداقة على الفيسبوك، فقبلت ومتكلمناش خالص غير من ثلاث شهور لما علقتله على بوست ليه، دخل بعتلي رسايل للتعارف، بردوا اسمه يوسف ضابط طيار من القاهرة قريب من سني بيشتغل في شركة طيران في إحدى دول الخليج وإن باباه أردني ومامته مصرية عايشة في إسكندرية بيبقى ييجي يزورها وباباه عايش في دولة خليجية رجل أعمال، نفس الحوار بردوا عايز يرتبط بمصرية زي مامته، طبعا الاسم بنبرة الصوت اللي أنا لسه تقريبًا فاكراها شكيت فيه، لإنه بدأ يحاول يأفور في الكلام سواء علاقة غير صحيحة، أو ضحكة كدة عالية كإنه بيقولي خلاص إنتي اتعلمتي ومش هعرف انصب عليكي المرة دي؟ أو إنه قالي فيه الأميرة موزة من دولة خليجية طلبته بالإسم يطلع معاها حفلة عاملاه على اليخت، وعشان فترة كورونا وشركة الطيران كانت بتخسر، فمجلس الإدارة خلاه يوافق إنه يطلع معاها، المهم حاول كتير معايا يخليني اغلط في الكلام عشان طبعا يبقى في إيده حاجة يهدد بيها بطريقة غير مباشرة، وحاول يخليني اثق فيه، وعزمني على افتتاح مكان في القاهرة وفرصة نتقابل لكن أنا رفضت. ولما فقد الأمل مني عملي بلوك. بعدها بشهر كدة نزلت تطبيق التوكتوك، لقيته باعتلي صداقة بنفس الصورة اللي كانت على أكونت الفيسبوك، فإتكدت إنه هو نفس النصاب بتاع قبل كده من سنين، عشان تطبيق التيكتوك بيتبعت فيه برقم الموبايل، ومش صدفة إنه كمان كان عارف صفحتي على الفيس، فلغيت طلب الصداقة وخلاص على كده.

ثامنًا: صور النصب الإلكتروني في عصر الرقمنة "الأسباب_ المكافحة"

أكد مؤتمر "كيوتو" الذي عقدته الأمم المتحدة في اليابان للوقاية من الجريمة من ٧ إلى ١٢ مارس ٢٠٢١ على مدى قلق المجتمع الدولي من الطابع المنظَم للجريمة العابر للقارات، ذلك في ظل الإستعمال المتزايد

للتكنولوچيا الحديثة من خوارزميات عبر الإنترنت وبرمجيات الروبوتات الذكية والويب المُظلم، حيث ترفع تلك الأشياء من التحديات التي تواجه إستراتيچيات مكافحة الجرائم المستحدثة(٤٦).

فقد وفرت الرقمنة فضاءات جديدة للمُعلِنين يستطيعون من خلالها البحث عن زبائنهم المستهدفين بطريقة أسهل وأكثر دقة. بذلك فإن الأمور أصبحت تصب أكثر في صالح الشركات المُعلِنة حيث أنهم لا يقومون فقط بتوجيه رسائلهم، بل أيضًا يتعرفون على مدى تأثير تلك الرسائل بسرعة أكبر، والميزة الأهم أنهم يتواصلون مع الزبائن في أي مكان وزمان بفضل "خاصية التزامن" التي أدخلت الشركات في عالم تواصلي جديد قائم على إمكانية التحدث مع الزبائن بسبب التكنولوچيا الحديثة التي تربط الهواتف الذكية بالإنترنت طوال اليوم، مما يساعد في وجود تغذية راجعة للجماهير تُسهل الدخول في علاقة جدية بين الطرفين(٤٧).

ويوجد عقد البيع الإلكتروني الذي له صورتان؛ (الصورة الأولى: بيع السلع المادية) يكون الاتفاق على النت بينما التسليم خارج النت يدًا بيد. (الصورة الثانية: بيع الخدمات) يكون الاتفاق على النت وأيضَا التسليم على النت(٤٨). لكن عند الدراسة الميدانية فقد وجدت الباحثة حالات لم يلتزم فيها البائع بهذا العقد الإلكتروني، وقام بالنصب على المشتري؛ ففي السلع المادية كان يتم التسليم لكن بمواصفات غير مطابقة لِما تم الاتفاق عليه، أو أنه يتم أخذ ثمن السلعة دون تسليمها. وفي بيع الخدمات كان يتم أخذ ثمن الخدمة دون تنفيذها.

(٤٦) سليم أحمد المصمودي: ٢٠٢٢، الاتجاهات الحديثة للوقاية من الجريمة: كيف تتجدّد المقاربات الكلاسيكية في العصر الرقمي؟، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي_ جامعة نايف العربية للعلوم الأمنية_ السعودية_ مجلد٤ عدد٢، ص١٧٠. https://doi.org/10.26735/MOEY2066

(٤٧) نور الدين هميسي، الوليد رفاس: ٢٠٢٣، عن عصر الإشهار الإلكتروني: سؤال النشأة، طفرة الاستهداف وثورة التصميم، مجلة الحكمة للدراسات الإعلامية والاتصالية_ مؤسسة كنوز الحكمة للنشر والتوزيع_ مجلة دولية ببريطانيا والجزائر_ مجلد١١ عدد١، ص ص١٩٣: ١٩٥. https://www.asjp.cerist.dz/index.php/en/article/217070

(٤٨) السيد أحمد السيد فوده: ٢٠٢٤، الإلتزام بالتسليم في البيع الإلكتروني بين القانون المدني والفقه الإسلامي، المجلة القانونية جامعة القاهرة كلية الحقوق فرع الخرطوم_ مجلد١٩ عدد٤، ص٢٤٤٥. 10.21608/jlaw.2024.341546

أيضًا تؤدي الهجمات السيبرانية على المستوى الشخصي للأفراد إلى خسائر مالية كبيرة، عن طريق الاحتيال المالي عبر الإنترنت بإستخدام برامج خبيثة تستهدف سرقة معلومات بطاقات الائتمان أو الحسابات المصرفية الشخصية(٤٩).

وجدير بالذِكر أن الدستور المصري لعام ٢٠١٤ في المادة ٦٩ قد نص على: الحكومة تتولى إنشاء هيئة وطنية للأمن السيبراني، تكون مختصة بتأمين المعلومات والبيانات وشبكات المعلومات من المخاطر الداخلية والخارجية. ومن أمثلة جرائم تقنية المعلومات التي جرمها قانون رقم ١٧٥ لسنة ٢٠١٨: (جرائم الاحتيال الإلكتروني التي تتم عن طريق استخدام الوسائل الإلكترونية مثل النت أو المحمول، جرائم التزوير الإلكتروني أي جرائم تزوير المحررات الإلكترونية مثل الفواتير والعقود، جرائم القرصنة الإلكترونية أي الدخول غير المشروع على الأنظمة المعلوماتية، جرائم القرصنة المالية سواء سرقة الأموال أو سرقة المعلومات المالية من على الأنظمة المعلوماتية)(٥٠).

مما سبق يُمكن إيجاز أن: العقود الأخيرة قد أحدثت تغيرات جذرية في صناعة الدفع، حيث يتم الآن استخدام وسائل الدفع الإلكترونية المختلفة مثل التحويلات والخصم والبطاقات، تلك الوسائل الإلكترونية قد زاحمت الخدمات المصرفية الورقية بشكل كبير حيث جعلتها تتخلف عن الرَكب. قد أدى ذلك إلى ظهور تكيُف كبير لإعتماد وتطبيق استخدام أجهزة الكمبيوتر الشخصية والمحمولة والأجهزة اللوحية والهواتف المحمولة والذكية والإنترنت والشبكات وما إلى ذلك، لتوفير خدمات مريحة وموثوقة وآمنه وسريعة للعملاء. أدى هذا إلى خطوة تالية في هذا التطور وهي أن تكتمل العلاقة بين البنك والعميل مع جهات فاعلة جديدة في سلسلة الدفع، حيث بدأت البنوك في تكثيف روابطها مع التجار في مجال التجارة الإلكترونية. لكن أيضًا في الوقت ذاته قد يجد مقدموا تلك الخدمات أن تلك الوساطة والشراكة قد أثارت مشاكل قانونية تخص معلومات حساب الدفع وخدمات بدء الدفع وتبادل بيانات الاعتماد من قِبل العملاء وتقاسم المسئولية بين مقدمي خدمات الدفع في سلسلة الدفع. وبهذا فإن السؤال الأكثر أهمية الآن هو: كيف يُمكن ضمان أمن المدفوعات في ظل هذه الظروف المتغيرة والبيئة الرقمية؟ هذا ما يثير مسألة

(٤٩) إيمان مرسي رزق النجار: ٢٠٢٤، الوعي الديني كآلية لمواجهة الهجمات السيبرانية في المملكة العربية السعودية (دراسة سوسيورقمية)، مجلة كلية الآداب جامعة الفيوم_ مجلد١٦ عدد١، ص٩٤٨. 10.21608/jfafu.2024.261953.2015

(٥٠) أحمد حسن أبوالحسن: ٢٠٢٤، مدى تأثير الرقمنة على خطورة الجرائم الاقتصادية، مجلة جامعة أسوان للعلوم الإنسانية_ مجلد٤ عدد١، ص ص٣٠، ٣٢. 10.21608/masuh.2024.338287

مصادقة جميع المشاركين في الدفع، وهي إحدى المشاكل الرئيسية التي يجب حلها عن طريق تعديل توجيه خدمات الدفع الإلكتروني، وهكذا فإن الأمر لازال يتعلق بالمستقبل لكي يتم تعيين النموذج أو النماذج التي توفر مصادقة قوية يُمكن أن تُصبح معيار عالمي لجميع المدفوعات(٥١).

والخلاصة فإنه من الجدير بالذِكر أن مكافحة الاحتيال باعتباره أحد أهم الجرائم الإلكترونية الحديثة، هي مهمة تستغرق وقتًا طويلًا ومكلفة؛ لأن الجهات الفاعلة السيئة تتطور باستمرار وتستغل الفرص الجديدة لاستغلال نقاط الضعف في أنظمة الحماية من الاحتيال والكشف عنها، بل المُلفت للنظر أن جهود التطوير ذاتها تؤدي إلى تفاقم المشكلة، على سبيل المثال: شرح تقنيات الكشف عن الاحتيال أو منعه في المجال العام، هذا من شأنه أن يزود المحتالين بالمعلومات اللازمة للتهرب من الكشف. وبالتالي تقع الأبحاث العلمية بين طرفي نقيض؛ هل تقوم بعملية الحد من تبادل الأفكار والنتائج البحثية، أم تقوم بنشرها ويستفيد منها المحتالون؟(٥٢).

تاسعًا: نتائج الدراسة

تبعًا لأهداف الدراسة وللإجابة على تساؤلاتها، يُمكن مناقشة النتائج وفقًا للمحاور التالية:

المحور الأول: البيانات الأساسية:

جدول رقم (١) :متغيِر النوع

الجُناة		
الفئات	مجموع التكرارات	النسبة المئوية
ذكر	٨	% ٤٠
أنثى	٢	% ١٠
غير معروف	١٠	% ٥٠
المجموع	٢٠	%١٠٠
الضحايا		
الفئات	مجموع التكرارات	النسبة المئوية
ذكر	٦	% ٣٠
أنثى	١٤	% ٧٠
المجموع	٢٠	%١٠٠

(51) Levente Kovács, Sandor David: 2016, Fraud risk in electronic payment transactions, Journal of Money Laundering Control _ Vol. 19 No. 2 _ Emerald. https://doi.org/10.1108/JMLC-09-2015-0039

(52) Abed Mutemi, Fernando Bacao: 2023, A numeric-based machine learning design for detecting organized retail fraud in digital marketplaces, Scientific Reports. https://doi.org/10.1038/s41598-023-38304-5

يوضح الجدول رقم (١) متغير نوع العينة سواء كانوا جُناة أو ضحايا. تنوه الباحثة أنها صنفت الجُناة ذكور أو إناث في حالة التأكد من ذلك بنسبة ١٠٠% ذلك عن طريق حديث الضحايا معهم صوتيًا أو رؤيتهم في مقابلة واقعية، أما إذا لم يتم ذلك فاعتبرت الباحثة أن متغير النوع غير معروف "حيث كان التواصل كتابيًا فقط عن طريق: مجموعات أو صفحات أو حسابات –صحيحة ومُهكرة– على شبكات التواصل الاجتماعي". أما بالنسبة لتصنيف الضحايا فيوجد تأكيد عليهم جميعًا بنسبة ١٠٠% أيضًا لأنهم هم من تكلموا مع الباحثة عن جريمة النصب التي حدثت معهم، وحتى في بعض الحالات التي سردها معارف الضحايا فقد كانوا مصدر ثقة لدى الباحثة.

وبذلك تكونت عينة الجُناة من (٥٠%) غير معروف جنسهم ذكور أو إناث أي نصف العينة، ذلك بسبب انتهاز الجُناة لفرصة إمكانية التواصل الخفي مع ضحاياهم خلف شاشات الأجهزة الإلكترونية. في حين ظهور الجُناة الذكور بنسبة (٤٠%) أي أربع أضعاف الجُناة من الإناث اللاتي ظهرن بنسبة (١٠%) فقط، مما يوضح أن طبيعة شخصية الذكور في الميل لإرتكاب جرائم النصب الإلكتروني أكبر بكثير من الإناث.

أما عن عينة الضحايا؛ فظهرت فيها الإناث في المرتبة الأولى بنسبة (٧٠%) وهي نسبة كبيرة بالمقارنة بنسبة الذكور (٣٠%) فقط، وربما يرجع ذلك إلى أن الإناث هدف أكبر للجُناه.

جدول رقم (٢) :متغيِر السن

الجُناة		
الفئات	مجموع التكرارات	النسبة المئوية
٢٣ : ٢٨ سنة	٢	١٠ %
غير معروف	١٨	٩٠ %
المجموع	٢٠	١٠٠%
الضحايا		
الفئات	مجموع التكرارات	النسبة المئوية
١٧ : ٢٠ سنة	٨	٤٠ %
٢٠ : ٣٠ سنة	٥	٢٥ %
٣٠ : ٤٠ سنة	٢	١٠ %
٤٠ : ٥٠ سنة	٢	١٠ %
٥٠ : ٦٠ سنة	٢	١٠ %
غير معروف	١	٥ %
المجموع	٢٠	١٠٠%

يوضح الجدول السابق متغير السن بالنسبة للجُناة والمجني عليهم، حيث جاء في المرتبة الأولى بنسبة (٩٠%) أن سن الجُناة غير معروف، ومن المؤكد أن ذلك يرجع إلى أن الجُناة يحاولون إخفاء بياناتهم الشخصية قدر الإمكان حتى لا يتوصل إليهم أحد. وفئة (٢٣ : ٢٨ سنة) بنسبة (١٠%) فقط.

أما الضحايا فتنوعت فئات سنهم لأنهم من قاموا بسرد حالة النصب فيذكرون أغلب بياناتهم الشخصية بشكل طبيعي. جاء في المرتبة الأولى فئة السن (١٧ : ٢٠ سنة) بنسبة (٤٠%) أي يقتربون من النصف تقريبًا، وتلك نسبة كبيرة ربما تعود إلى أن ذلك السن الصغير يكون الأقل خبرة والأكثر ثقة بالآخرين، مما يجعلهم يقعون فريسة سهلة للنصب الإلكتروني. والفئة الثانية (٢٠ : ٣٠ سنة) بنسبة (٢٥%) وتلك أيضًا نسبة ليست قليلة، ربما يعود سبب وقوعهم في النصب إلى نفس سبب الفئة الأولى، لكن عددهم أقل قليلًا ربما بسبب أن بعضهم قد أخذ الخبرة والحذر لأنهم في سن أكبر. تساوت بعد ذلك فئات: (٣٠ : ٤٠ سنة) (٤٠ : ٥٠ سنة) (٥٠ : ٦٠ سنة) بنسبة (١٠%) فقط لكل فئة، وتلك نسبة صغيرة، ربما يرجع ذلك إلى زيادة الخبرة لديهم في التعامل مع الأشخاص على الإنترنت. وظهرت حالة واحدة في فئة غير معروف السن بنسبة (٥%) فقط.

جدول رقم (٣):متغيِر التعليم

الجُناة		
الفئات	مجموع التكرارات	النسبة المئوية
تعليم عالي	١	٥ %
غير معروف	١٩	٩٥ %
المجموع	٢٠	١٠٠%
الضحايا		
الفئات	مجموع التكرارات	النسبة المئوية
في الثانوية العامة	٣	١٥ %
طالب جامعي	٤	٢٠ %
تعليم عالي	٥	٢٥ %
تعليم متوسط	٣	١٥ %
دبلوم	٣	١٥ %
غير معروف	٢	١٠ %
المجموع	٢٠	١٠٠%

يوضح الجدول رقم (٣) متغير التعليم بالنسبة لأفراد العينة؛ حيث كان هذا المتغير غير معروف بنسبة (٩٥%) عند الجُناة، في حين ظهور التعليم العالي بنسبة (٥%) فقط لديهم.

أما عن الضحايا؛ فقد جاء في المرتبة الأولى متغير تعليم عالي بنسبة (٢٥%)، وتقارب في النسبة معه طالب جامعي (٢٠%). تساوي في المرتبة الثالثة ثلاث متغيرات (في الثانوية العامة) (تعليم متوسط) (دبلوم) بنسبة (١٥%). بينما كان هناك نسبة (١٠%) غير معروف تعليمهم. وبذلك فإنه عند قراءة الجدول السابق يتضح: أن الجميع معروضون للنصب الإلكتروني بإختلاف تعليمهم.

جدول رقم (٤) :متغيِر الحالة الاجتماعية

الجُناة		
الفئات	مجموع التكرارات	النسبة المئوية
مخطوب	١	% ٥
متزوج	٣	% ١٥
غير معروف	١٦	% ٨٠
المجموع	٢٠	%١٠٠
الضحايا		
الفئات	مجموع التكرارات	النسبة المئوية
أعزب	٨	% ٤٠
متزوج	٧	% ٣٥
غير معروف	٥	% ٢٥
المجموع	٢٠	%١٠٠

تناول الجدول رقم (٤) متغير الحالة الاجتماعية للعينة؛ حيث جاء في المرتبة الأولى بنسبة (٨٠%) لدى الجُناة أنهم غير معروف حالتهم الاجتماعية، وهذه نسبة طبيعية لأن الجناة يخفون شخصياتهم الحقيقية. بينما ظهر متغير متزوج بنسة (١٥%)، ومتغير مخطوب بنسبة (٥%).

وعن الضحايا؛ فتقاربت نسبة أعزب (٤٠%) مع نسبة متزوج (٣٥%) مما يدل على أن الجميع من الممكن أن يتعرضون للنصب الإلكتروني. بينما ظهرت نسبة (٢٥%) غير معروف حالتهم الاجتماعية.

جدول رقم (٥) :متغيِر الحالة الاقتصادية

الجُناة		
الفئات	مجموع التكرارات	النسبة المئوية
عالية	١	٥ %
متوسطة	١	٥ %
غير معروف	١٨	٩٠ %
المجموع	٢٠	١٠٠%
الضحايا		
الفئات	مجموع التكرارات	النسبة المئوية
متوسطة	٧	٣٥ %
غير معروف	١٣	٦٥ %
المجموع	٢٠	١٠٠%

يعرض الجدول السابق رقم (٥) متغير الحالة الاقتصادية لدى أفراد العينة، وكالمعتاد فإن المرتبة الأولى لدى الجُناة فئة غير معروف مستواهم الاقتصادي حيث ظهر هذا المتغير بنسبة (٩٠%). في حين تساوت الفئتين (عالية) (متوسطة) بنسبة (٥%).

ذلك في حين أيضًا أن متغير الحالة الاقتصادية لدى الضحايا كان بنسبة (٦٥%) غير معروف، ذلك لأن الضحايا اعتبروا هذا المتغير من البيانات الخاصة ولم يرغبوا الإفصاح عنه. وظهر في المرتبة الثانية بنسبة (٣٥%) فئة الحالة الاقتصادية المتوسطة، وهي المستوى الشائع لدى أغلب الشعب المصري.

المحور الثاني: كيفية حدوث جريمة النصب الإكتروني في العصر الرقمي:

جدول رقم (٦):متغيِر علاقة الجُناة بالضحايا

الفئات	مجموع التكرارات	النسبة المئوية
شخص على Whats App.	١	٥ %
شخص على فيسبوك	٨	٤٠ %
شخص على انستجرام	١	٥ %
شخص على الموبايل	٢	١٠ %
شخص على النت	٦	٣٠ %
أصدقاء ومعارف	٢	١٠ %
المجموع	٢٠	١٠٠%

يعرض الجدول رقم (٦) متغير علاقة الجُناة بضحاياهم، حيث تعددت أنواع تلك العلاقات. فجاء في المرتبة الأولى أن الجاني كان شخص على فيسبوك، ظهر ذلك بنسبة (٤٠%). بينما ذَكر (٣٠%) من الضحايا أن الجاني كان شخص على النت، وقالوا أن التعارف كان على شبكة تواصل اجتماعي ولم يحددوا أي شبكة. وجاء في المرتبة الثالثة أن الجاني كان شخص على الموبايل وتم التواصل بمكالمة صوتية، أو أن الجاني كان من أصدقاء ومعارف الضحايا، ظهر هذان المتغيران بنسبة (١٠%) بين أفراد العينة. بينما ظهر في المرتبة الأخيرة بنسبة (٥%)، أن الجاني كان شخص على تطبيق: Whats App. أو انستجرام.

جدول رقم (٧) :متغيِر طُرق النصب الإلكتروني

الفئات	مجموع التكرارات	النسبة المئوية
التسوق الإلكتروني	٥	% ٢٥
طلب الزواج	٢	% ١٠
فرصة عمل	٧	% ٣٥
بنك افتراضي على الإنترنت	١	% ٥
الخداع بوجود حالة مرضية	٢	% ١٠
رسالة لتحديث البيانات البنكية	١	% ٥
الخداع بتعديل درجات الثانوية العامة	١	% ٥
الخداع بالفوز بمبلغ مادي	١	% ٥
المجموع	٢٠	%١٠٠

أوضح الجدول السابق رقم (٧) عدة طرق استخدمها الجُناة في النصب على ضحاياهم. جاء في المرتبة الأولى بنسبة (٣٥%) أن الجناة عرضوا فرص عمل على شبكات التواصل الاجتماعي، تمثلت تلك الفرص في: إعلان للعمل بمرتب مُغري، تسويق لمنتجات، تشغيل أموال. ظهر في المرتبة الثانية بنسبة (٢٥%) عمليات التسوق الإلكتروني، حيث تمثل ذلك في الشراء عن طريق الإنترنت أو ترويج للسلع. وتساوى في المرتبة الثالثة بنسبة (١٠%) طرق: طلب الزواج للتقرب من الضحايا ثم النصب عليهن، الخداع بوجود حالة مرضية تحتاج أموال للعلاج. وجاء في المرتبة الأخيرة بنسبة (٥%) طرق: بنك افتراضي على الإنترنت، رسالة على الموبايل لتحديث البيانات البنكية، الخداع بتعديل درجات الثانوية

العامة، الخداع بالفوز بمبلغ مادي لأن رقم موبايل الضحية مميز. وبهذا فعند تحليل هذا الجدول، يتضح أن النصابون دائمًا ما يبحثون عن متطلبات واحتياجات الضحايا لكي يخدعوهم بتلبيتها، ومن ثَم ينصبون عليهم بكل سهولة.

جدول رقم (٨) :متغيِر كيفية كسب الجُناة ثقة الضحايا

الفئات	مجموع التكرارات	النسبة المئوية
خلق العلاقات الاجتماعية	٢	٥ %
خداع الجاني ضحيتة بأن حالتة الاقتصادية مرتفعة للغاية	٣	٧.٥ %
تبادل الصور الشخصية	١	٢.٥ %
الحوار على الخاص	١٥	٣٧.٥ %
المستندات الرسمية	٣	٧.٥ %
المقابلة وجهًا لوجه	٣	٧.٥ %
منح الضحية أرباح قبل النصب الإلكتروني	٣	٧.٥ %
اختيار التوقيت المناسب للنصب الإلكتروني	١	٢.٥ %
عرض إعلانات السلع على الجروبات الكبيرة على شبكات التواصل الاجتماعي	٢	٥ %
عرض صور فوتوغرافية	٣	٧.٥ %
تهكير صفحة على شبكة تواصل اجتماعي وإرسال رسائل منها للأفراد الموجودين عليها	٢	٥ %
عرض لقطات شاشة Screenshot	٢	٥ %
المجموع	٤٠	%١٠٠

يوضح الجدول السابق استخدام الجُناة طرق عديدة لكي يكسبوا ثقة ضحاياهم ومن ثَم يستطيعوا النصب عليهم بإستغلال تلك الثقة، وبالتالي ظهر أن مجموع التكرارات (٤٠) أكبر من عدد الحالات (٢٠)، ذلك لأن الجُناة كانوا يستخدمون أكثر من طريقة لمحاولة كسب ثقة ضحيتهم والتقرب منها. فجاء في المرتبة الأولى الحوار على الخاص (كتابة، فيديو، صوت) بنسبة (٣٧%)، حيث أن جميع الجُناة تكلموا مع ضحاياهم بشكل شخصي عن طريق شبكات التواصل الاجتماعي أو مكالمات الموبايل. تساوى بعد ذلك بعض الطرق بنسبة (٧.٥%) كالتالي: (خداع الجاني ضحيتة بأن حالتة الاقتصادية مرتفعة للغاية)،

(المستندات الرسمية) سواء عرض بطاقة شخصية أو الباسبور أو الإشاعات طبية أو عقد شراكة أو طلب رقم جلوس لجنة الامتحان، (المقابلة وجهًا لوجه)، (منح الضحية أرباح قبل النصب الإلكتروني) سواء كانت عالية جدًا أو عادية لإثبات صدق النية، (عرض صور فوتوغرافية) سواء كانت لمرضى لكسب تعاطف الضحايا أو لشُغل سابق له كغرف نوم ليظهر مهارته في العمل أو لمكان الشغل على أرض الواقع لإثبات الجدية. أيضًا تساوت في المرتبة الثالثة نسبة بعض الطرق (٥%) كالتالي: (خلق العلاقات الاجتماعية) سواء عن طريق التعارف بين عائلة الجاني والضحية أو العزومات والصداقة، (عرض إعلانات السلع على الجروبات الكبيرة على شبكات التواصل الاجتماعي)، (تهكير صفحة على شبكة تواصل اجتماعي وإرسال رسائل منها للأفراد الموجودين عليها)، (عرض لقطات شاشة Screenshot) لمكاسب عملاء سابقين أو أيضًا في إحدى الحالات ظهر الخداع بنتائج ثانوية عامة تم تعديلها. وفي المرتبة الأخيرة بنسبة (٢.٥%) ظهرت طريقتين: (تبادل الصور الشخصية)، (اختيار التوقيت المناسب للنصب الإلكتروني) كتوقيت معروف إن فيه عروض خصم كنهاية السنة أو عروض يوم الجمعة.

جدول رقم (٩) :متغيِر كيفية إخفاء الجُناة هويتهم الحقيقية

الفئات	مجموع التكرارات	النسبة المئوية
التعارف بالضحية عن طريق شبكات التواصل الاجتماعي	١٤	٧٠ %
إخفاء محل الإقامة الحقيقي	١	٥ %
التواصل مع الضحية عن طريق مكالمة موبايل	٢	١٠ %
لم يتم إخفاء الهوية الحقيقية	٣	١٥ %
المجموع	٢٠	١٠٠%

يوضح الجدول رقم (٩) الطرق التي استخدمها الجُناة لكي يخفوا هويتهم الحقيقة أمام ضحاياهم؛ حيث ظهر في المرتبة الأولى بنسبة تصل إلى أكبر من النصف (٧٠%) أن التعارف بالضحية كان عن طريق شبكات التواصل الاجتماعي، وتحليل ذلك أن شبكات التواصل بإختلاف أشكالها تُعَد بيئة خصبة لإخفاء الجاني نفسه خلف ذلك العالم الإفتراضي، ثم يظهر أمام الضحية بأي حيل وأكاذيب يريد أن يخدعها بها، فغالبًا لن يكون أمام الضحية اختيار سوى تصديق الجاني ولو بشكل مؤقت حتى يثبت عكس ما يقول، وهذا يمنح الجاني وقتًا يستطيع من خلاله إتمام عملية النصب الإلكتروني. جاء في المرتبة الثانية بنسبة (١٥%) أنه لم يتم إخفاء الهوية الحقيقية، نظرًا لأن الجُناه كانوا أصدقاء ومعارف للضحايا، فكانوا

يعرفون بعضهم البعض من قبل النصب الإلكتروني، مما جعل الضحايا يثقون في الجُناة بشكل أكبر وقد استغل الجُناة ذلك. تقاربت بعد ذلك في النسبة بعد الطرق الأخرى: التواصل مع الضحية عن طريق مكالمة موبايل، بنسبة (١٠%)، إخفاء محل الإقامة الحقيقي وإظهار محل إقامة غير صحيح، ذلك كان بنسبة (٥%) من أفراد العينة.

جدول رقم (١٠) :متغيِر إتمام عملية النصب الإلكتروني

الفئات	مجموع التكرارات	النسبة المئوية
تم النصب الإلكتروني	١٩	% ٩٥
لم يتم النصب الإلكتروني	١	% ٥
المجموع	٢٠	%١٠٠

أوضح الجدول رقم (١٠) أنه قد تم النصب الإلكتروني بنسبة (٩٥%) من بين أفراد العينة، في حين أن نسبة (٥%) فقط لم يتم النصب الإلكتروني فيها من بين أفراد العينة. وتنوه الباحثة أن تلك النسبة كانت غير مقصودة عند اختيار العينة من الأشخاص الذين تعرضوا لنصب إلكتروني، بل كان ذلك بشكل طبيعي، مما يدل على أن أغلب حالات النصب الإلكتروني ينجح فيها الجُناة في الإيقاع بالضحايا، مما ينذر بخطورة تلك الظاهرة.

المحور الثالث: الآثار الاجتماعية للنصب الإلكتروني

جدول رقم (١١) :متغيِر حجم خسائر الضحايا

الفئات	مجموع التكرارات	النسبة المئوية
أموال	١٨	% ٨٥.٧
بيع ممتلكات	٢	% ٩.٥
شراء أدوية	١	% ٤.٨
المجموع	٢١	%١٠٠

يوضح الجدول رقم (١١) حجم خسائر الضحايا، ومجموع التكررات أكبر من عدد الحالات لأن هناك حالة كانت خسائرها أكثر من شيء واحد. جاء في المرتبة الأولى بنسبة (٨٥.٧%) خسارة الأموال بإختلاف عدد تلك الأموال بين أفراد العينة، ذلك لأن الهدف الأساسي لمعظم النصابون هو الحصول

على الأموال؛ كانت تلك الأموال (غير معلومة العدد، ٥٠٠ ألف جنيه، ١٠٠ ألف جنيه، ٣٥ ألف جنيه، ١٨ ألف جنيه، "٧ : ١٠" آلاف جنيه، ٣ آلاف جنيه، ١٣٠٠ جنيه أو أقل). في المرتبة الثانية بنسبة (٩.٥%) بيع ممتلكات مثل: سيارة وأثاث من المنزل، بهدف أيضًا توفير الأموال للجُناة. والمرتبة الأخيرة بنسبة (٤.٨%) شراء أدوية لأن الجُناة خدعوا الضحايا بوجود مرضى.

جدول رقم (١٢) :متغيِر استرداد الضحايا لأموالهم من الجُناة

الفئات	مجموع التكرارات	النسبة المئوية
لم يتم استرداد أي أموال	١٨	% ٩٤.٧
استرداد ٢٠ ألف من أصل ١٢٠ ألف	١	% ٥.٣
المجموع	١٩	%١٠٠

يتناول الجدول رقم (١٢) متغير استرداد الضحايا لأموالهم من الجُناة، وبذلك فإن هذا الجدول خاص بالضحايا الذين تم إتمام النصب الإلكتروني عليهم فقط وعددهم (١٩) حالة من أصل (٢٠) حيث أن هناك حالة لم يتم النصب عليها. جاء في المرتبة الأولى بنسبة (٩٤.٧%) أن الضحايا لم يستردوا أي أموال. في حين أن هناك نسبة (٥.٣%) تم استرداد (٢٠ ألف) من أصل (١٢٠ ألف) من زوج ابنة الجاني لإن المجني عليه ذهب إلى منزلها وأحدث لها مشاكل بسبب النصب من أبيها. هذا يدل أن النصاب عندما يحقق هدفه في النصب على الضحية، فإنه يستحيل أن يُرجع الأموال التي حصل عليها أبدًا بغير طُرق القوة والإجبار.

جدول رقم (١٣):متغيِر رد فعل الضحايا بعد النصب الإلكتروني عليهم

الفئات	مجموع التكرارات	النسبة المئوية
محاولة الانتحار	١	% ٥.٣
إبلاغ الشرطة الإلكترونية	٦	% ٣١.٦
محاولة إنهاء الشراكة المالية مع الجُناة	٢	% ١٠.٥
محاولة أخذ المشورة من الأصدقاء	١	% ٥.٣
نُصح الناس لعدم الوقوع في النصب الإلكتروني	٤	% ٢١
محاولة الوصول إلى الجاني أو معلومات عنه	٢	% ١٠.٥
لم يتم فعل شيء	٣	% ١٥.٨
المجموع	١٩	%١٠٠

الجدول رقم (١٣) يوضح متغيِر رد فعل الضحايا (١٩ حالة) بعد النصب الإلكتروني عليهم؛ حيث اختلف تأثير عملية النصب الإلكتروني على الضحايا حسب كل حالة. جاء في المرتبة الأولى بنسبة (٣١.٦%) أن الضحايا قاموا بإبلاغ الشرطة الإلكترونية، مما يبين وجود الوعي لدى الأشخاص في محاولة ردع الجاني واسترداد الحق منه في إطار الضبط الاجتماعي. وفي المرتبة الثانية بنسبة (٢١%) قام الضحايا بنُصح الناس لعدم الوقوع في النصب الإلكتروني، ذلك لكي يفيدوا الناس بخبرتهم التي تعرضوا لها. في المرتبة الثالثة بنسبة (١٥.٨%) لم يتم فعل شيء، ذلك بسبب أن الجُناة يضعون الضحايا في مواقف يصعب فيها على الضحية أن تتخذ موقف إيجابي وتقوم بالإبلاغ عن الجاني لأن هذا يعرض الضحايا للإحراج أو أن المبلغ المنصوب فيه لم يكن كبير فلا يستحق عناء محاولة استرجاعه، وبالتأكيد هذا يجعل الجُناة يتمادوا في عمليات نصب إلكتروني جديدة. تساوى بعد ذلك بنسبة (١٠.٥%) محاولة إنهاء الشراكة المالية مع الجُناة، محاولة الوصول إلى الجاني أو معلومات عنه عن طريق عمل مشاكل عند أهله أو محاولة التواصل معه من رقم موبايل آخر. وتساوى في المرتبة الأخيرة بنسبة (٥.٣%) متغيري: محاولة الانتحار بسبب التعرض لضغط شديد من الجاني، محاولة أخذ المشورة من الأصدقاء.

وبشكل عام أصبح الضحايا لا يثقون في أي شخص حتى لو كان الأقرب بالنسبة لهم، قالت إحدى الضحايا (لازم نتأكد من أي كلام خاصة التبرعات، مش أي كلام نصدقة وخلاص)، أصبحوا حذرين أكثر، قالت إحدى الضحايا (بعد كده ممنوع أرن على أي رقم مجهول الهوية، وكنت المفروض اتجهه لجهة إصدار الفيزا واستفسر منهم على الرسالة اللي وصلتني).

جدول رقم (١٤):متغيِر القبض على الجُناة

الفئات	مجموع التكرارات	النسبة المئوية
تم الإمساك بالجاني	٢	% ١٠
لم يتم الإمساك بالجاني (على الرغم من إتمام النصب الإلكتروني)	١٧	% ٨٥
لم يتم الإمساك بالجاني (لعدم إتمام النصب الإلكتروني)	١	% ٥
المجموع	٢٠	%١٠٠

تناول الجدول رقم (١٤) متغيِر القبض على الجُناة؛ جاء في المرتبة الأولى بنسبة (٨٥%) أنه لم يتم الإمساك بالجاني (على الرغم من إتمام النصب الإلكتروني). وفي المرتبة الثانية بنسبة (١٠%) فقط أنه قد تم الإمساك بالجاني، في حين أن نسبة (٥%) لم يتم الإمساك بالجاني (لعدم إتمام النصب الإلكتروني).

عاشرًا: توصيات الدرسة

خلصت الدراسة إلى بعض التوصيات تبعًا لأهدافها وللإجابة على تساؤلها الأخير: ما التدابير الأمنية لتجنب الوقوع في فخ النصب الإلكتروني؟ ويُمكن مناقشة تلك التوصيات وفقًا لأربع محاور كما يلي:

المحور الأول: توصيات خاصة بالفرد "الشخص الذي يستخدم الإنترنت"

حظى هذا المحور بأغلب التوصيات لأن الفرد هو هدف الجاني في المقام الأول، فقد أوضحت الدراسة الميدانية أن الجاني يقوم بالنصب الإلكتروني على فرد بعينة وليس مجموعة أفراد في الوقت ذاته، ثم يكمل مساره في النصب الإلكتروني على فرد آخر، وهكذا.. إلخ. فيمكن عرض تلك التوصيات كما يلي:

١- عدم الاستجابة المباشرة للأصدقاء على صفحات التواصل الاجتماعي عندما يطلبون تحويل أموال، إلا بعد التأكد من شخصيتهم عن طريق محادثتهم صوتيًا على رقم موبايلهم الشخصي مثلًا. لأن ما يحدث الآن هو تهكير صفحات الأفراد وانتحال شخصياتهم، ثم يتم إرسال رسالة نصية للأصدقاء يطلبون فيها أموال بعد خداعهم بوجود ظروف طارئة، ويرسلون رقم موبايل للضحية للتحويل عليه رقم كارت شحن أو تحويل أموال على محفظة كاش.

٢- عدم الثقة الكاملة في الأشخاص عند التواصل عن طريق تطبيقات مشهورة ذات ثقة للناس مثل Facebook و Telegram لأن الكثير من الجُناة يستغلون الشعبية الكبيرة لتلك التطبيقات لكي يطمئنوا الضحايا ويخدعوهم ثم ينصبون عليهم. أيضا ليست كل الإعلانات حقيقية حتى وإن كانت على تلك المواقع المشهورة.

٣- عدم الرد على الأرقام التي يتم إرسال رسائل منها، مثل: (عزيز العميل لقد تم إيقاف حساب كارت الفيزا برجاء الاتصال بنا) أو (عزيزي العميل تم إيقاف حسابكم البنكي موقتا لتحديث برجأ الإتصال) مع ملاحظة أن الرسالة النصية بها أخطاء لغوية لا يصح أن تصدر عن جهة مسئولة كالبنك.

٤- عدم تصديق الأشخاص الذين يتصلون على الموبايل أو التليفون الأرضي، عندما يقولون مثلًا: (رقمك مميز وفاز بجائزة) وللعِلم من ينصب باستخدام الموبايل، غالبًا يكون مسجله باسم كيان كبير على "برامج البحث عن رقم الموبايل" لخداع الضحية، إحدى الضحايا قالت: (الرقم اللي نصب عليا كان متسجل على برنامج تروكولر باسم البنك المركزي المصري).

٥- عدم الاطمئنان الكلي للأشخاص الذين يعرضون فرص عمل على الإنترنت –خاصة من يقومون بعرض عائد مادي كبير– ثم يدفعون ربح مقابل هذا العمل. فغالبًا يلتزم النصابون بتسليم الضحايا أرباحهم في البداية لحين اكتساب الثقة، فيزيدوا من استثماراتهم، هنا تتم عملية النصب على توَسُع. لذلك عندما نجد عرض مقابل عائد مادي كبير نظير العمل، يجب التحري جيدًا قبل الدخول في هذا العمل.

٦- الحذر من دفع أي أموال لأي شخص على شبكات التواصل الاجتماعي. فبعض النصابون يحاولون انتهاز فرصة أن بعض الطلبة يبحثون عن فرص عمل على النت، فيحاولون اصطيادهم بفرص وهمية لأعمال بسيطة لا تحتاج إلى خبرة ولا وقت مثل عرض إعلانات لمنتجات شركة، قالت إحدى الضحايا (فيه ناس على النت كانوا قالولي ادفع مائة جنيه تأمين، وفيه كانوا قالولي ادفع ألف جنيه وبترجعلك بعد كده عشان نضمن الجدية في العمل).

٧- معروف أن الشعب المصري شعب عاطفي، يُمكن استدراجه بسهوله لدفع تبرعات لحالات إنسانية (تحتاج مثلًا علاج أو عمليات أو عروسة تتزوج) ويتم عرض صور مؤثرة تدعم صِدق النصاب، فيجب التأكد من مثل تلك الحالات.

٨- عدم عرض بيانات الفيزا لأي شخص (حيث تكررت حالات النصب على الأفراد ذوي التعليم المتوسط وتحت المتوسط وكبار السن، بأن تصلهم رسالة من رقم موبايل يطلب الرقم القومي ورقم الفيزا والرقم السري، لأنه تم إيقاف حسابهم البنكي، فيردون برسالة فيها البيانات المطلوبة، فيتفاجئوا برسالة من البنك بأنه تم سحب كل رصيدهم) (بل إن إحدى الضحايا اتصل به رقم مجهول وقاله إنه من البنك، وقاله اسمه كامل والنُص الأول من رقم الفيزا، وطلب منه يكمل باقي الرقم، ويقوله الرقم السري، ثم سرق ١١ ألف الموجودين بالفيزا وقفل الموبايل) أيضًا لا يوجد شيء اسمه إنك كسبت، ونريد بيانات الفيزا لتحويل المبلغ.

٩- الحذر من الدخول على أي Link حتى لو كان شغل، قالت إحدى الضحايا (مفيش أي حاجة بقيت مضمونة وومكن يكون هاكر).

١٠- محاولة التعرف على كل جديد، لأن النصب يكون أسهل عندما تكون الضحية قليلة الخبرة في مجال التكنولوجيا.

١١- عند الشراء إلكترونيًا يجب عدم دفع أي أموال إلا بعد استلام السلعة.

١٢- محاولة الاعتماد على النفس قدر الإمكان حتى لو الشخص هيبدأ بمشروع صغير لكنه سوف يكون مضمون في قبضة يده. قال أحد الضحايا (اتعلمت إن بعد كده اشغل فلوسي بنفسي، مش اديها لحد يشغلهالي) وقال آخر (اللي عايز يخسر حد يشاركه).

١٣- عندما نجد شخص يحاول دائمًا إظهار إنه غني جدًا، وفجأة يطلب أموال بأي مبرر ما، فالأغلب إنه نصاب.

١٤- عدم الذهاب إلى مقابلات عمل في أماكن مجهولة وغير مشهورة. قالت إحدى الضحايا بعد مرورها بتجربة سيئة: (كنت بتعلق بأي إعلان عمل على النت عشان كنت محتاجة الشغل، وكانوا بيلعبوا بأعصابي ويقولولي فيه interview لكن الصح إني ابحث في أماكن اعرفها أحسن).

١٥- تطبيقات التعارف مكان خصب لتواجد النصابون. قالت إحدى الفتيات (دخل واحد كلمني بلغة انجليزية وقالي إنه من ألمانيا لكن عايش في إنجلترا، وأخد رقم موبايلي وبعت لي رقمه لنكمل التعارف Whats App. بعدها كلمني رقم دولي بيقولي على شغل بسيط عن طريق الموبايل إني اعمل إعجابات كتقييم لفنادق ومطاعم ومحلات وهيدفعولي من ٦٠ جنيه : ٥٠٠٠ ألاف جنية يوميًا).

١٦- لكسب ثقة الضحايا يقوم الجناة بعرض بعض تفاصيل عن حياتهم الشخصية ليوهموا الضحايا أنهم أصبحوا أصدقاء والعلاقة أصبحت أكبر من شغل فقط. قالت إحدى الضحايا (النصابة كانت حريصة أوي إنها تبان لطيفة معايا، وحكيت كتير عن تفاصيل حياتها، وسمعت كمان تفاصيل عن حياتي). لذلك يجب الحرص قدر الإمكان عند التعامل مع البائعون.

المحور الثاني: توصيات خاصة بالأسرة

١ تربية الأبناء على ثقافة استرداد الحقوق عند التعرض لأي أذى إلكتروني، حتى يتبرمج عقل الطفل على ذلك منذ الصغر.

٢ تدعيم ثقة الأبناء بأنفسهم، حتى لا يستسلمون لمطالب النصابون على الإنترنت، حيث أظهرت الدراسة الميدانية أن هناك ضحايا لا يقومون حتى بأبسط الأشياء كأن يبتعدون عن الجناة ولا يردون عليهم، بل أنهم يدفعون الأموال للنصابون لشراء صمتهم عن شيء يهددونهم به.

المحور الثالث: توصيات خاصة با لمجتمع

١- صياغة وتفعيل القوانين المواكبة للتطور التكنولوچي السريع، من أجل حماية المستهلكين عند الشراء عن طريق الإنترنت، مثل:

- استرجاع ثمن السلعة إذا كانت غير مطابقة للمواصفات التي كانت معروضة قبل الشراء.
- تتبع النصابين والمحتالين حتى القبض عليهم، وتطبيق العقوبة الصارمة التي يستحقونها.

المحور الرابع: توصيات خاصة بالضحايا

١- عدم اهتزاز الثقة بالنفس مهما حاول الجاني إضعاف الضحية. لأن النصابون لا يكتفيون بأذى الضحية مرة واحدة، بل يتهمون الضحايا بأنهم هم المؤذيون حتى يجعلوا الضحية تلقي اللوم على نفسها، ثم تستسلم لطلبات الجاني الذي يقوم بالنصب عليها مرات عديدة.

قائمة المصادر والمراجع

1) Abed Mutemi, Fernando Bacao: 2023, A numeric-based machine learning design for detecting organized retail fraud in digital marketplaces, Scientific Reports. https://doi.org/10.1038/s41598-023-38304-5

2) Adaora Immaculata Muoghalu, Jisike Jude Okonkwo, Amalachukwu Chijindu Ananwude: 2018, Effect of electronic banking related fraud on deposit money banks financial performance in Nigeria, Discovery Publication _ 54 (276). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305555

3) Aisha Abdallah, Mohd Aizaini Maarof, Anazida Zainal: 2016, Fraud detection system: A survey, Journal of Network and Computer Applications _ Volume 68 _ Elsevier. https://doi.org/10.1016/j.jnca.2016.04.007

4) Amaefule I.A, Onu F.U: 2019, Prevalence of Electronic Fraud in Nigeria Banking System, International Journal of Computer Trends and Technology _ Volume 67 Issue 3. https://www.researchgate.net/profile/I-

Amaefule/publication/334053572_Prevalence_of_Electronic_Fraud_in_Nigeria_Banking_System/links/5efee28692851c52d6137dee/Prevalence-of-Electronic-Fraud-in-Nigeria-Banking-System.pdf

5) Babatunde Moses Ololade, Mary Kehinde Salawu, Aderemi Daniel Adekanmi: 2020, E-Fraud in Nigerian Banks: Why and How?, Journal of Financial Risk Management _ Vol.9 No.3 _ Scientific Research Publishing. 10.4236/jfrm.2020.93012

6) Braimah, O.J & Okonkwo, I.A: 2016, Statistical Monitoring (SM) of Electronic Fraud Occurring in Nigerian Banks, Advances in Multidisciplinary Research Journal _ Vol. 2 No. 3. https://www.researchgate.net/profile/Joseph-Braimah/publication/328702484_Statistical_Monitoring_SM_of_Electronic_Fraud_Occurring_in_Nigerian_Banks/links/5bdca9e1299bf1124fb56410/Statistical-Monitoring-SM-of-Electronic-Fraud-Occurring-in-Nigerian-Banks.pdf

7) Charles Emeka Nwobia, Patrick Anayo Adigwe, Gideon Kasie Ezu, John Nonso Okoye: 2020, Electronic Fraud and Performance of Deposit Money Banks in Nigeria: 2008-2018, International Journal of Business and Management _ Vol. 15 _ No. 6 _ Canadian Center of Science and Education. 10.5539/ijbm.v15n6p126

8) Damaris Karimi Mwabu: 2013, Factors influencing electronic fraud in the banking industry in Kenya:a case of Kenya commercial bank central region, College of Humanities and Social Sciences _ Faculty of Education _ University of Nairobi. http://erepository.uonbi.ac.ke/handle/11295/60487

9) Daria Kibets, Olena Lepei, Oleksii Prokopenko, Alina Chorna, Mykola Shelukhin: 2019, Anti-Fraud Technologies in E-Banking, Journal of legal, ethical and regulatory issues _ Volume 22 special Issue 2 _ Hein on line. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jnlolletl22&div=168&id=&page=

10) Emad Abu-Shanab, Salam Matalqa: 2015, Security and Fraud Issues of E-banking, International Journal of Computer Networks and Applications _ Volume 2, Issue 4 _ EverScience Publications. https://d1wqtxts1xzle7.cloudfront.net/53498558/Abu-Shanab___Matalqa_2015-libre.pdf?1497418633=&response-content-disposition=inline%3B+filename%3DSecurity_and_Fraud_Issues_of_E_banking.pdf&Expires=1722432407&Signature=FQtislwcVY9yU~4DJJ-JXdbJrZPiXAEzMcSWITDPaE84k~a-NTgLtT7U9Po69q9dZJ7gA2H8IbfTWFqhqDrWdjQriLSbwr2HJscxXtpBlYn3jCr0vqTEkHksHsa19JypwYy0kQXuvbl9pVcIZki0gzt3RuZZVVBJAy2rcpej68JoPDmFMlY5v3PhvWm~JKNPxXvemPmD52pjmp8C2TMgWLJZK5R8OJEjtH7ck3SXPxMAFV815sW~CjoO-mSmQQ~7iAtJGeYRJcugkXZJ8TMbbtNFyFQ38bC-73XeKAcLM6mWzQVeZDuvlILzJndnoeur5pN6TloB~SH5Tnm8xCEL1g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

11) Folowosele Folarin Akinwale, Ikpefan Ochei Ailemen, Isibor Areghan: 2022, Electronic fraud: an emerging cause of bank failure in Nigerian deposit money banks, Journal of Money Laundering Control _ Volume 25 Issue 1 _ Emerald Insight. https://doi.org/10.1108/JMLC-01-2021-0009

12) Gabriel Preti Santiago, Adriano C. M. Pereira, Roberto Hirata, Jr: 2015, A modeling approach for credit card fraud detection in electronic payment services, ACM Digital Library _ Association for Computing Machinery. https://dl.acm.org/doi/abs/10.1145/2695664.2695990

13) Ghazioui Hinda: 2023, Electronic fraud from changing the concept to changing the protection, International journal of legal and political research _ Volume 7 Issue 3. https://www.asjp.cerist.dz/en/downArticle/473/7/3/237838

14) Ibanichuka E.A.L, Oko I. A.:2019, Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria, International Journal of Advanced Academic Research | Management Practice _ Vol. 5 _ Issue 4. https://www.ijaar.org/articles/Volume5-Number4/Management-Practice/ijaar-mp-v5n4-apr19-p2.pdf

15) Ilya Levin, Dan Mamlok: 2021, Culture and Society in the Digital Age, MDPI Journals _ Volume 12 Issue 2. https://www.mdpi.com/2078-2489/12/2/68

16) José Felipe Júnior, Adriano Pereira, Wagner Meira Júnior, Adriano Veloso: 2012, Methodology for fraud detection in electronic transactions, ACM Digital Library _ Association for Computing Machinery. https://doi.org/10.1145/2382636.2382697

17) Levente Kovács, Sandor David: 2016, Fraud risk in electronic payment transactions, Journal of Money Laundering Control _ Vol. 19 No. 2 _ Emerald. https://doi.org/10.1108/JMLC-09-2015-0039

18) Lina Fernandes: 2013, Fraud electronic payment transactions: threats and countermeasures, Asia Pacific Journal of Marketing & Management Review _ Vol.2 (3). https://www.researchgate.net/profile/Mohamed-Mourad-Lafifi/post/Is-it-possible-to-help-me-with-similar-sources-or-research-for-the-purpose-of-completing-my-research-projects-on-the-development-of-electronic-paymen/attachment/5cb7642b3843b01b9b9abf38/AS%3A748730219257856%401555522603426/download/FRAUD+IN+ELECTRONIC+PAYMENT+TRANSACTIONS+_+THREATS+AND+COUNTERMEASURES.pdf

19) Ludivia Hernandez Aros, Luisa Ximena Bustamante Molano, Fernando Gutierrez-Portela, John Johver Moreno Hernandez, Mario Samuel Rodríguez Barrero: 2024, Financial fraud detection through the application of machine learning techniques: a literature review, humanities and social sciences communications. https://doi.org/10.1057/s41599-024-03606-0

20) María M. Moreno-Fernandez, Fernando Blanco, Pablo Garaizar, Helena Matute: 2017, Fishing for phishers _ Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud, Computers in Human Behavior _ Volume 69 _ Elsevier. https://doi.org/10.1016/j.chb.2016.12.044

21) OGBONNA, Kelechukwu Stanley & OKARO, Celestine & IGWE, Elizabeth Ihuoma: 2019, Electronic fraud and credit facilitation of banks in Nigeria, Journal of Accounting Information and Innovation _ Vol.5 _ No.10. https://www.researchgate.net/profile/Kelechukwu-Ogbonna/publication/336903627_ELECTRONIC_FRAUD_AND_CREDIT_FACILITATION_OF_BANKS_IN_NIGERIA/links/5dba18534585151435d615b6/ELECTRONIC-FRAUD-AND-CREDIT-FACILITATION-OF-BANKS-IN-NIGERIA.pdf

22) Olubunmi Alabi, Amos David: 2022, Model for forecasting electronic fraud threats on selected electronic payment channels using linear regression, International Journal of Information Technology _ Volume 14 _ Springer Nature. https://doi.org/10.1007/s41870-022-00939-4

23) Oludayo Tade, Oluwatosin Adeniyi: 2020, Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem, International Journal of Offender Therapy and Comparative Criminology _ Volume 64 Issue 16 _ Sage Journals. https://doi.org/10.1177/0306624X20928028

24) Shewangu Dzomira:2014, Electronic fraud (cyber fraud) risk in the banking industry _ Zimbabwe, Risk governance & control: financial markets & institutions _ Volume 4 _ Issue 2. https://www.researchgate.net/profile/Shewangu-Dzomira-2/publication/282281593_Electronic_fraud_cyber_fraud_risk_in_the_banking_industry_Zimbabwe/links/560a58a908ae576ce63fc422/Electronic-fraud-cyber-fraud-risk-in-the-banking-industry-Zimbabwe.pdf

25) Tade, Oludayo & Adeniyi, Oluwatosin: 2017, Automated teller machine fraud in south-west Nigeria: Victim typologies, victimisation strategies and fraud prevention, Journal of Payments Strategy & Systems _ Volume 11 Number 1 _ Henry Stewart Publications. https://www.ingentaconnect.com/content/hsp/jpss/2017/00000011/00000001/art00011

26) Valentin-Stelian Bădescu: 2013, Fraud in electronic commerce, Perspectives of Business Law Journal _ Issue No: 02 _ Central and eastern European online library. https://www.ceeol.com/search/article-detail?id=477497

27) Wang Haoxiang, S. Smys: 2021, A Survey on Digital Fraud Risk Control Management by Automatic Case Management System, Journal of Electrical Engineering and Automation _ Vol.03 No.01. https://web.archive.org/web/20210511004002id_/https://irojournals.com/iroeea/V3/I1/01.pdf

28) Yen-Wu Ti, Yu-Yen Hsin, Tian-Shyr Dai, Ming-Chuan Huang, Liang-Chih Liu: 2022, Feature generation and contribution comparison for electronic fraud detection, Scientific reports. https://doi.org/10.1038/s41598-022-22130-2

29) Yue Guo, Yongchuan Bao, Barnes J. Stuart, Khuong Le-Nguyen: 2017, To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce, Wiley online library _ Volume 28 Issue 2. https://doi.org/10.1111/isj.12144

30) Zahoor Ahmed Soomro, Javed Ahmed, Mahmood Hussain Shah, Khalil Khoumbati: 2019, Investigating identity fraud management practices in e-tail sector: a systematic review, Journal of Enterprise Information Management _ Volume 32 Issue 2 _ Emerald Publishing Limited. https://www.emerald.com/insight/content/doi/10.1108/jeim-06-2018-0110/full/html

٣١) أحمد حسن أبوالحسن: ٢٠٢٤، مدى تأثير الرقمنة على خطورة الجرائم الاقتصادية، مجلة جامعة أسوان للعلوم الإنسانية_ مجلد٤ عدد١، ٣٢. 10.21608/masuh.2024.338287

٣٢) إلهام عبدالرحمن إبراهيم شحاته: ٢٠٢٠، نهج جديد للإعلان في العصر الرقمي، مجلة العمارة والفنون والعلوم الإنسانية_ الجمعية العربية للحضارة والفنون الإسلامية_ مجلد٥ عدد٢٠. 10.21608/mjaf.2019.13613.1213

٣٣) أماني رضا أبوالمعارف سباع: ٢٠٢١، أداء المعلم الجامعي في ضوء متطلبات العصر الرقمي، مجلة العلوم التربوية_ كلية التربية بقنا_ مجلد ٤٦ عدد ٤٦. 10.21608/maeq.2021.77805.1027

٣٤) إيمان مرسي رزق النجار: ٢٠٢٤، الوعي الديني كآلية لمواجهة الهجمات السيبرانية في المملكة العربية السعودية (دراسة سوسيورقمية)، مجلة كلية الآداب جامعة الفيوم_ مجلد١٦ عدد١. 10.21608/jfafu.2024.261953.2015

٣٥) بن ققة سمراء، نوي نور الهدى: ٢٠٢٣، علاقة مواقع التواصل الاجتماعي بالنصب والاحتيال من وجهة نظر طلبة الجامعين "دراسة ميدانية على عينة من طلبة علوم الاعلام والاتصال جامعة قاصدي مرباح ورقلة"، جامعة قاصدي مرباح ورقلة_ كلية العلوم الإنسانية والاجتماعية_ قسم علوم الإعلام والاتصال. https://dspace.univ-ouargla.dz/jspui/handle/123456789/34553

٣٦) تهاني الخطيب: ٢٠٢٤، إشكالية الهوية العربية الإسلامية في العصر الرقمي، دراسات العلوم الإنسانية والإجتماعية_ مجلد٥١ عدد٤_ جامعة الأردن. https://dsr.ju.edu.jo/djournals/index.php/Hum/article/view/566/1807

٣٧) حملاوي مهتور: ٢٠٢٤، الفلسفة أهميتها ومآلها في العصر الرقمي، مجلة التطوير العلمي للدراسات والبحوث_ مجلد٥ عدد١٨. https://doi.org/10.61212/jsd/222

٣٨) راوية عبدالحميد إبراهيم، محمد جابر محمود، رشاد ابوالمجد مصطفى: ٢٠٢٣، العصر الرقمي: مفهومه وخصائصه ومتطلباته وتأثيره على قيم المواطنة، مجلة العلوم التربوية_ كلية التربية بقنا_ جامعة جنوب الوادي_ عدد٥٥ ج١. https://maeq.journals.ekb.eg/article_299655_426478877b90a48f5022b74a041e968b.pdf

٣٩) ُسرية علي أمان آل جميل: ٢٠٢٣، تحديات استخدام وسائل التواصل الاجتماعي الحديثة على مؤسسة الأسرة في القرن الحادي والعشرين– دراسة وصفية، مجلة العلوم الإنسانية والإجتماعية_ مجلد٧ عدد٩. https://doi.org/10.26389/AJSRP.L060623

٤٠) سليم أحمد المصمودي: ٢٠٢٢، الاتجاهات الحديثة للوقاية من الجريمة: كيف تتجدّد المقاربات الكلاسيكية في العصر الرقمي؟، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي_ جامعة نايف العربية للعلوم الأمنية_ السعودية_ مجلد٤ عدد٢. https://doi.org/10.26735/MOEY2066

٤١) السيد أحمد السيد فوده: ٢٠٢٤، الإلتزام بالتسليم في البيع الإلكتروني بين القانون المدني والفقه الإسلامي، المجلة القانونية جامعة القاهرة كلية الحقوق فرع الخرطوم_ مجلد١٩ عدد٤. 10.21608/jlaw.2024.341546

٤٢) عبدالوهاب عبدالكريم محمد المبارك: ٢٠٢٣، إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك، المجلة القانونية_ مجلد١٥ عدد٨_ كلية الحقوق فرع الخرطوم جامعة القاهرة. 10.21608/JLAW.2023.286561

٤٣) فايزة عبيد، نريمان حريسي: ٢٠٢٢، الإدارة الإلكترونية ودورها في العصر الرقمي، مذكرات العلوم الإنسانية_ قسم علوم الإعلام والإتصال_ كلية العلوم الإنسانية والاجتماعية_ جامعة العربي التبسي. http//localhost:8080/jspui/handle/123456789/5225

٤٤) محمد جبريل جبريل: ٢٠٢٣، الإطار التشريعي لمواجهة الثورة الرقمية من الوجهة الجنائية دراسة تحليلية مقارنة، مجلة الدراسات القانونية والاقتصادية_ مجلد٩ عدد٣. 10.21608/jdl.2023.230278.1201

٤٥) محمود موسى زياد: ٢٠٢٤، الفلسفة وتحديات العصر الرقمي، مجلة التطوير العلمي للدراسات والبحوث_ مجلد٥ عدد١٧. https://doi.org/10.61212/jsd/196

٤٦) محمود هلال عبدالباسط عبدالقادر: ٢٠٢٢، الثقافة الرقمية للأبناء بين الرفاهية والحتمية في العصر الرقمي "رؤية تربوية"، المجلة التربوية_ كلية التربية جامعة سوهاج_ عدد٩٥ ج١. 10.21608/edusohag.2022.214740

٤٧) مفيدة طاير: ٢٠٢٠، مقومات وتحديات تشكيل الهوية الرقمية للمؤسسة في العصر الرقمي، المجلة العلمية للتكنولوجيا وعلوم الإعاقة_ مجلد٢ عدد٤. 10.21608/SKJE.2020.38254.1003

٤٨) منى تركي شمخي: ٢٠٢٣، أخلاقيات التواصل في العصر الرقمي وانعكاسها على تواصل الجمهور، مجلة آداب المستنصرية_ عدد١٠٤.
https://amm.uomustansiriyah.edu.iq/index.php/mustansiriyah/article/download/1123/960

٤٩) نور الدين هميسي، الوليد رفاس: ٢٠٢٣، عن عصر الإشهار الإلكتروني: سؤال النشأة، طفرة الاستهداف وثورة التصميم، مجلة الحكمة للدراسات الإعلامية والاتصالية_ مؤسسة كنوز الحكمة للنشر والتوزيع_ مجلة دولية ببريطانيا والجزائر_ مجلد١١ عدد١.
https://www.asjp.cerist.dz/index.php/en/article/217070

٥٠) ولاء أسعد عبدالجواد عبدالحليم: ٢٠٢٤، الكتابة الإبداعية في العصر الرقمي "الفرص والتحديات"، المجلة العلمية لكلية الآداب جامعة أسيوط_ مجلد٣١ عدد٨٩. 10.21608/AAKJ.2023.249423.1604

٥١) وليم هوسلي، ترجمة: وليد رشاد زكي: ٢٠٢١، المجتمع في العصر الرقمي: منظور تفاعلي، المجلة المصرية للعلوم الاجتماعية والسلوكية_ مؤسسة تواصل للدراسات والتوعية الثقافية.
https://ejsbs.journals.ekb.eg/article_203573_f918e1dc44078e1da167060b11fed84c.pdf

٥٢) يحيى إبراهيم دهشان: ٢٠٢٤، الحماية الجنائية للمستهلك الإلكتروني، الدوريات المصرية.
https://journals.ekb.eg/article_352592_0.html