جامعة تكريت

كلية التربية للعلوم الصرفة

قسم علوم الحياة

البحث الأكاديمي بعنوان:

التهديدات الرقمية في المجتمع العراقي

(دراسة تحليلية لظواهر النصب الإلكتروني وضعف الوعي الرقمي)

إعداد الطالب: مؤمن خلف عبدالله العبيدي

البريد الإلكتروني: ibnsamh97@gmail.com

رقم الهاتف: 07824313633

السنة الدراسية: ٢٠٢٤-٢٠٢٥

فهرس المحتويات

الملخص:

يواجه المجتمع العراقي تحديات متزايدة في ميدان الأمن الرقمي، تتجلى في انتشار ظواهر النصب الإلكتروني، سرقة الحسابات، واستغلال الخدمات الحكومية من قبل ضعاف النفوس. ويأتي هذا البحث ليسلّط الضوء على هذه الظواهر من خلال تحليل أسبابها، واستعراض أمثلة حقيقية، ومقارنة الأوضاع الحالية مع تجارب أخرى، بهدف تقديم حلول واقعية قابلة للتطبيق تعزز من الوعي الرقمي وتحمي المواطن العراقي من التهديدات المتنامية.

الكلمات المفتاحية:

الوعي الرقمي، الأمن السيبراني، الجرائم الإلكترونية، النصب الإلكتروني، المجتمع العراقي، الاحتيال الرقمي، مواقع وهمية، زين كاش، الاختراق، الشائعات الرقمية.

Abstract:

Iraqi society is facing increasing challenges in the field of digital security, manifested in the spread of electronic fraud, account hacking, and the exploitation of government services by scammers. This research aims to highlight these phenomena by analyzing their causes, reviewing real-life examples, and comparing the current situation with other international experiences to offer practical and applicable solutions that enhance digital awareness and protect Iraqi citizens.

Keywords:

Digital Awareness, Cybersecurity, Electronic Crimes, Online Fraud, Iraqi Society, Digital Scam, Fake Websites, Zain Cash, Account Hacking, Digital Deception.

المقدمة

شهد العراق في السنوات الأخيرة تطورًا ملحوظًا في استخدام الإنترنت، وأصبح الأفراد يعتمدون عليه في مختلف جوانب الحياة مثل التعليم، التوظيف، التواصل، وحتى الخدمات الحكومية. هذا التحول الرقمي السريع، ورغم ما يحمله من إيجابيات، إلا أنه لم يُواكب بوعي مجتمعي كافٍ تجاه أخطار الفضاء السيبراني.

الكثير من المواطنين لا يمتلكون المعرفة الكافية بكيفية استخدام الإنترنت بطريقة آمنة، مما جعلهم عرضة لعمليات نصب واحتيال إلكتروني. سواء عبر مواقع مزيفة، أو صفحات تنتحل صفة جهات حكومية، أو تطبيقات خادعة، أصبح الإنترنت بيئة خصبة للمحتالين الذين يستغلون ثغرات الوعي والثقة الزائدة للمواطن.

يهدف هذا البحث إلى تسليط الضوء على أبرز التهديدات الرقمية التي تواجه المجتمع العراقي، مع تحليل نماذج حقيقية من عمليات النصب المنتشرة، واستعراض العوامل المؤدية لها. كما سيتم اقتراح مجموعة من الحلول الواقعية والمستدامة التي تساعد على رفع الوعي الرقمي وتعزيز ثقافة الأمن السيبراني في المجتمع.

الفصل الأول: ضعف الوعي الرقمي في المجتمع العراقي

من أبرز أسباب انتشار الجرائم الإلكترونية في العراق هو ضعف الوعي الرقمي لدى غالبية المواطنين. فالكثير من المستخدمين يتعاملون مع الإنترنت بعفوية مفرطة دون معرفة بأساسيات الأمان السيبراني، مما يجعلهم هدفًا سهلًا للمخترقين والمحتالين.

تتجلى مظاهر ضعف الوعي في عدة صور، منها:

- إدخال البيانات الشخصية في مواقع مشبوهة دون تحقق من مصداقيتها.

- تحميل تطبيقات من مصادر غير رسمية.

- مشاركة معلومات حساسة عبر منصات غير آمنة.

- تصديق منشورات تحمل شعارات مؤسسات حكومية أو تعليمية مزيفة دون تدقيق.

وما يزيد الأمر سوءًا هو غياب برامج توعية رسمية، أو محتوى تعليمي ممنهج يوضح للمواطن كيف يحمي نفسه رقميًا، سواء في المناهج المدرسية أو الحملات الإعلامية. كما أن كثيرًا من العائلات لا تولي اهتمامًا لتوعية أبنائها، ما يؤدي إلى تعرضهم لمخاطر متعددة.

ضعف الثقافة الرقمية لا يشمل فقط الأفراد، بل يمتد أحيانًا إلى بعض الموظفين في المؤسسات، حيث يقومون بمشاركة روابط غير موثوقة، أو يخزنون معلومات حساسة في أجهزة غير محمية.

ولذلك، يعتبر الوعي الرقمي أساسًا لا يمكن تجاهله في ظل التحول الرقمي الحالي، ويجب أن يكون على رأس أولويات أي خطة تطوير مجتمعي أو تعليمية.

الفصل الثاني: مظاهر النصب الإلكتروني

تنتشر مظاهر النصب الإلكتروني في المجتمع العراقي بشكل واسع، خصوصًا مع تزايد استخدام وسائل التواصل الاجتماعي وتطبيقات الدفع الإلكتروني. ويعتمد المحتالون على أساليب نفسية وتقنية بسيطة لكنها فعالة، تستغل قلة وعي المستخدم أو حاجته المالية.

من أبرز صور النصب:

١. **مواقع شحن الألعاب المزيفة:**

يتم إنشاء صفحات إلكترونية شبيهة بمواقع ألعاب شهيرة مثل PUBG أو Free Fire ، تطلب من المستخدم إدخال اسم الحساب وكلمة المرور. وبمجرد إدخال البيانات يتم الاستيلاء على الحساب وبيعه أو استخدامه لأغراض غير شرعية.

٢. **قنوات تيليجرام تقدم "دورات" أو "تداول:"**

تدّعي بعض القنوات أنها تقدم فرص ربح من التداول أو الكورسات، مقابل مبلغ يُرسل عبر "زين كاش". وبعد الدفع، يبدأ التماطل أو يُغلق الحساب دون تقديم أي خدمة.

٣. **صفحات تنتحل صفة مؤسسات حكومية:**

خاصةً بعد إعلان وزارة التجارة عن خدمة تحديث البطاقة التموينية، ظهرت صفحات مزيفة تطلب من الناس إرسال صور ومعلومات شخصية مقابل ١٠ آلاف دينار، رغم أن العملية الأصلية تحتاج إلى قراءة البطاقة بجهاز NICF ولا يمكن إتمامها عن بعد.

٤. **صفحات تبيع خدمات وهمية:**

مثل فتح حسابات مصرفية، أو استخراج بطاقات كي كارد، أو تقديم وظائف حكومية "مضمونة"، كلها تحت مسميات مغرية مقابل رسوم بسيطة، وبعد الدفع لا يحصل المواطن على شيء.

هذه الأساليب البسيطة تعتمد على الاستدراج النفسي وسرعة القرار، في ظل غياب تدقيق من المواطن، ما يجعل آلاف الأشخاص ضحية في كل شهر.

الفصل الثالث: استغلال الخدمات الحكومية

واحدة من أخطر أنواع النصب الإلكتروني هي **استغلال اسم وخدمات مؤسسات الدولة**، واللعب على وعي المواطن وثقته بكل ما يرتبط بالحكومة.

ظهر هذا النوع بقوة مع رقمنة بعض الخدمات مثل البطاقة التموينية، الرعاية الاجتماعية، أو تحديث بيانات الناخبين. ويقوم المحتالون بإنشاء صفحات تحمل شعارات وزارات رسمية، ويطلبون من المواطنين إرسال معلوماتهم مقابل مبلغ بسيط عبر زين كاش.

أمثلة:

- بعد إعلان وزارة التجارة العراقية عن إمكانية تحديث البطاقة التموينية إلكترونيًا، ظهرت صفحات تطلب من المواطن ١٠ آلاف دينار لتحديث البيانات، رغم أن العملية الأصلية لا تتم إلا من خلال جهاز خاص لقراءة البطاقة ولا يمكن تنفيذها عن بُعد.
- صفحات تدّعي فتح تسجيل للرعاية الاجتماعية، وتطلب من المواطن رقم هاتفه، صورته، وأحيانًا بطاقة السكن، وتجمع بيانات تُستخدم لاحقًا في النصب أو الابتزاز.
- بعض النصابين يستخدمون أرقام مكاتب تحويل أموال حقيقية لإخفاء هويتهم. فترسل الأموال باسم شخص غريب لا يعرف عن الموضوع شيئًا، وبعدها يُغلق الحساب أو يُحظر الشخص.

هذا النوع من النصب يستغل المواطن البسيط الذي يبحث عن تسهيل حياته أو الحصول على حقوقه، وغالبًا ما يدفع المبلغ دون تحقق لأن المبلغ يبدو بسيطًا... لكن الضرر النفسي أكبر بكثير.

الحل هنا ليس فقط في وعي المستخدم، بل في تفعيل رقابة إلكترونية صارمة، وإطلاق حملات حكومية توعية حقيقية توضح للناس كيف يتعاملون مع الخدمات الإلكترونية الرسمية.

الفصل الرابع: ضعف القوانين والتشريعات

رغم الانتشار الواسع لجرائم النصب الإلكتروني والاحتيال الرقمي في العراق، إلا أن الإطار القانوني لمواكبة هذا التطور ما يزال **ضعيفًا وبطيئًا**، سواء من حيث التشريع أو التنفيذ.

أبرز الإشكالات القانونية:

١. **غياب قانون شامل للجرائم الإلكترونية:**

العراق حتى الآن لا يمتلك قانونًا متكاملًا خاصًا بالجريمة الإلكترونية، بل تُعامل القضايا الرقمية ضمن قوانين عامة قد لا تتناسب مع طبيعة الجريمة التقنية.

٢. **صعوبة تعقّب المحتالين:**

الكثير من عمليات النصب تتم عبر أرقام وهمية، أو باستخدام VPN لإخفاء الموقع، ما يجعل الوصول إلى الجناة أمرًا معقدًا تقنيًا ويأخذ وقتًا طويلًا، ويؤدي غالبًا إلى حفظ الشكوى لعدم كفاية الأدلة.

٣. **قلة التخصص لدى الأجهزة الأمنية:**

رغم وجود وحدات مكافحة جرائم إلكترونية، إلا أن هذه الوحدات تعاني من نقص الكوادر التقنية والتجهيزات، ما يجعل أغلب البلاغات تُواجه بالتأجيل أو الإهمال.

٤. **ضعف وعي القضاء بطبيعة الجرائم الرقمية:**

بعض القضاة غير مطلعين على تفاصيل الجرائم الإلكترونية، وبالتالي قد لا تُفهم القضية بشكل تقني دقيق، مما يؤدي إلى ضعف الأحكام أو عدم التجريم من الأساس.

أمثلة من الواقع:

- شخص يقدّم شكوى على قناة تليجرام نصب عليه بـ زين كاش... لكن لا يتم ملاحقة الجاني لعدم وجود بيانات حقيقية.
- ضحية احتيال رقمي يُطلب منه تقديم دليل تقني يصعب توفيره بدون خبرة رقمية أو أدوات متخصصة.

الحل يبدأ من تشريع قانون عصري للجريمة الإلكترونية، يشمل:

- عقوبات واضحة
- آليات تبليغ سريعة
- تدريب كوادر أمنية وقضائية
- شراكة مع شركات الاتصالات والمنصات العالمية (مثل تيليجرام، فيسبوك، إلخ) لتعقّب الجناة

الفصل الخامس: الإعلام والتكنولوجيا في تعزيز أو تهديد الوعي الرقمي

يلعب الإعلام دورًا مزدوجًا في قضية الوعي الرقمي:

فهو إما أن يكون أداة توعية قوية تساعد المجتمع على كشف المحتالين وأساليبهم، أو يكون وسيلة تضليل غير مباشرة عبر نشر معلومات خاطئة أو محتوى غير دقيق.

أولًا: الإعلام كوسيلة توعية

بعض القنوات والمنصات العراقية (مثل البرامج الصباحية أو الفقرات التقنية في الفضائيات) بدأت بتسليط الضوء على قضايا النصب الإلكتروني، من خلال:

- استضافة ضحايا لعرض قصصهم.
- استشارة خبراء أمن سيبراني لشرح الأساليب المستخدمة.
- التحذير من صفحات وهمية وتطبيقات خطيرة.

لكن رغم هذه المحاولات، تبقى التغطية محدودة وغير منهجية، وغالبًا موسمية فقط بعد حدوث ضرر جماعي كبير.

ثانيًا: الإعلام كمصدر خطر

بالمقابل، هناك صفحات إعلامية ومؤثرون رقميون يشاركون روابط أو يروّجون لتطبيقات وخدمات بدون تحقق من مصداقيتها، ما يؤدي إلى:

- نشر روابط تحميل خطيرة

- الإعلان عن دورات استثمارية أو تداول مزيفة
- تضخيم فرص الربح السريع بدون وعي

كما أن بعض الصفحات تساهم في تكرار محتوى مسروق أو قديم، مما يجعل المستخدم لا يفرّق بين الحقيقي والمزيف.

ثالثًا: ضعف استخدام التكنولوجيا في الحماية

العراق لا يزال يعتمد على أساليب تقليدية في التبليغ عن الجرائم الإلكترونية، بينما في دول أخرى:

- هناك تطبيقات ذكية للتبليغ الفوري
- أنظمة تنبيه فوري عند محاولة الدخول لحسابات غير مألوفة
- حملات توعية إلكترونية تصل للناس عبر SMS أو الإعلانات الرسمية في المواقع

الخلاصة:

الإعلام يجب أن يتحول إلى خط الدفاع الأول ضد الجريمة الرقمية، وأن تكون هناك شراكة حقيقية بين الإعلام والجهات الحكومية لإطلاق حملات توعوية منتظمة، وتوفير محتوى رقمي موثوق بلغة بسيطة ومفهومة.

الفصل السادس: دراسات حالة من الواقع العراقي

لفهم حجم الخطر الحقيقي للتهديدات الرقمية، من المهم عرض حالات حقيقية حدثت لمواطنين عراقيين، تكشف كيف يتم استغلال الناس تحت مسميات مغرية.

الحالة الأولى: شحن لعبةPUBG

أحد الطلاب الجامعيين أراد شحن شدّات للعبة PUBG عبر رابط أرسله له صديق على تيليجرام.

الرابط بدا رسميًا، وكان يحمل شعار اللعبة، وطلب منه إدخال اسم الحساب وكلمة المرور.

بعد ٥ دقائق، تم اختراق الحساب بالكامل، وتم بيعه لاحقًا لشخص آخر، ولم يتمكن من استرجاعه رغم المحاولات.

تبين لاحقًا أن الرابط هو **نسخة مزيّفة من موقع الشحن** صُمم فقط لسرقة الحسابات.

الحالة الثانية: دورة تعليم تداول وهمية

شاب آخر شاهد إعلانًا على فيسبوك لقناة تقدم دورة تداول العملات الرقمية مقابل ١٥ ألف دينار عبر زين كاش.

تم دفع المبلغ، وتم وعده بدخول جروب خاص في تيليجرام، لكنه لم يُضف أبدًا.

وعند التواصل مع الرقم الذي استلم التحويل، اكتشف أنه رقم يعود لمكتب تحويل لا يعرف شيئًا عن الشخص.

بكل بساطة، النصاب استخدم "رقم شخص آخر" كواجهة، ثم حظره.

الحالة الثالثة: تحديث البطاقة التموينية

امرأة في بغداد شاهدت إعلانًا يطلب ١٠ آلاف دينار لتحديث البطاقة التموينية "عن بعد."

أرسلت المبلغ والمستمسكات عبر واتساب، ثم تم حظرها.

عند المراجعة تبين أن التحديث لا يتم إلا عبر جهاز خاص في مراكز رسمية، وأن كل ما جرى هو **نصب مكشوف**.

ماذا نستنتج من هذه الحالات؟

- المحتالون يغيّرون الأسلوب لكن النية واحدة: استغلال الثقة والجهل.
- أغلب الضحايا لا يبلّغون الجهات الرسمية، إما لليأس أو الخجل.
- عدم وجود طريقة سهلة للتبليغ يجعل هؤلاء المحتالين يكررون نفس الجريمة مع ضحايا جدد.

الفصل السابع: الحلول والتوصيات

بعد استعراض حجم التحديات الرقمية والنماذج الواقعية للنصب الإلكتروني في العراق، لا بد من وضع مجموعة من **الحلول الواقعية والقابلة للتطبيق**، على مستوى الدولة والمجتمع والأفراد.

أولًا: على مستوى الحكومة والمؤسسات الرسمية

١. **تشريع قانون شامل للجرائم الإلكترونية:**

قانون واضح يحدد العقوبات، طرق التبليغ، وآليات ملاحقة الجناة.

٢. **إطلاق منصة وطنية للتبليغ الإلكتروني:**

تطبيق رسمي على الهاتف يتيح لأي مواطن التبليغ عن عمليات نصب إلكتروني بسهولة وسرية.

٣. **التعاون مع شركات الاتصالات:**

لمنع تكرار استخدام نفس الأرقام أو الحسابات في عمليات النصب.

٤. **رقابة على الصفحات المزيفة:**

بالتعاون مع فيسبوك وتيليجرام لحظر الصفحات التي تنتحل صفات رسمية أو تروّج للنصب.

ثانيًا: على مستوى التعليم والمجتمع

١. **إدخال مادة "الوعي الرقمي" في المدارس والجامعات:**

تعليم الطلاب كيفية استخدام الإنترنت بأمان، والتعرف على أساليب النصب.

٢. **ورش عمل وتدريب في الأحياء والمراكز الشبابية:**

بإشراف منظمات المجتمع المدني، خاصة في المناطق الفقيرة أو ذات التعليم المنخفض.

٣. **إطلاق حملات توعوية عبر الإعلام:**

برامج أسبوعية أو مقاطع قصيرة تحذر من أشهر طرق النصب وكيفية الحماية منها.

ثالثًا: على مستوى الفرد

١. **عدم الوثوق بأي رابط أو صفحة تطلب معلومات شخصية أو مالية.**

٢. **تفعيل المصادقة الثنائية (Two-Factor Authentication)** للحسابات.

٣. **استخدام تطبيقات من المتاجر الرسمية فقط.**

٤. **نشر الوعي بين الأهل والأصدقاء، وعدم السكوت عند التعرّض للنصب.**

التوصية النهائية:

بناء **ثقافة رقمية واعية** هو مسؤولية جماعية تبدأ من كل فرد.

المعرفة الرقمية أصبحت ضرورة يومية، تمامًا كمعرفة استخدام المال أو الطرق.

ومن دونها، يبقى المواطن العراقي عرضة لموجات من الاستغلال والاحتيال.

الخاتمة

لقد أظهر هذا البحث بوضوح أن التهديدات الرقمية التي تواجه المجتمع العراقي لم تعد مجرد حالات فردية، بل أصبحت **ظاهرة اجتماعية خطيرة** تهدد الأمن الرقمي للمواطن والمؤسسات على حد سواء.

من خلال استعراض مظاهر النصب الإلكتروني، وتحليل نماذج حقيقية من الواقع، تبين أن غياب الوعي الرقمي، وضعف القوانين، وغياب الرقابة التكنولوجية، كلها عوامل تشكل بيئة خصبة لازدهار هذه الجرائم.

كما أن الإهمال في التعليم والتثقيف الرقمي فاقم من حجم المشكلة، خصوصًا في ظل اعتماد متزايد على الإنترنت في الخدمات الحكومية والحياتية اليومية.

إن الطريق نحو مجتمع رقمي آمن يتطلب تظافر الجهود بين:

- المواطن
- الجهات الحكومية
- الإعلام
- والمؤسسات التعليمية

فقط من خلال التوعية والتشريع والتقنية، يمكن الحد من هذه الظواهر وبناء مجتمع رقمي واعٍ ومحصّن.

المراجع

1. عبد الله، س. (2023). *الأمن السيبراني في العراق* .مجلة الدراسات الأمنية.

2. وزارة الداخلية العراقية. (2024). *تقرير الجرائم الإلكترونية السنوي*.

3. منظمة اليونسكو. (2022). *التثقيف الرقمي في الشرق الأوسط وشمال أفريقيا* .

4. الهيئة الوطنية للاتصالات والإعلام. (2023). *دليل الاستخدام الآمن للإنترنت*.

5. Al-Jazeera Tech. (2023). "Cybercrime Trends in the Arab World".

6. Iraq Digital Report. (2024). *Cybersecurity in Government Services*.