جامعة محمد خيضر بسكرة
كلية العلوم الإنسانية و الاجتماعية
قسم العلوم الإنسانية

مذكرة ماستر

ميدان : العلوم الإنسانية
الفرع :علوم الإعلام و الاتصال
التخصص: سمعي بصري

رقم: أدخل رقم تسلسل المذكرة

إعداد الطالب:
نخال صبرين

يوم://

الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي و علاقته بالثقافة الرقمية(دراسة مسحية لعينة من مستخدمي بريدي موب)

لجنة المناقشة:

د.منوبية قسمية	أ. مح أ	جامعة محمد خيضر بسكرة	رئيس
أ.دسراي سعاد	أ. مح أ	جامعة محمد خيضر بسكرة	مناقش
صونية قوراري	أ. مح أ	جامعة محمد خيضر بسكرة	مقرر

السنة الجامعية:2024-2025

الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEU
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE Med KHIDER BISKRA
FACULTE DES SCIENCES HUMAINES ET SOCIALES
Département de l'information de communication
et de bibliotéconomie

وزارة التعليم العالي و البحث العلمي
جامعة محمد خيضربسكرة
كية العلوم الإنسانية والاجتماعية
قسم الإعلام والاتصال وعلم المكتبات
2025الرقم: /ق.ع.إ/

2025 ماي 26بسكرة في:

اسم ولقب الأستاذ المشرف :قوراري صونية

الرتبة : استاذة محاضرة رتبة أ

المؤسسة الأصلية : جامعة محمد خيضر بسكرة

الموضوع: إذن بالإيداع

أنا الممضي أسفله الأستاذ (ة) قوراري صونية وبصفتي مشرفا على مذكرة الماستر للطالبة

1- نخال صبرين

في تخصص: سمعي بصري

والموسومة ب: الاحتيال الالكتروني عبر مواقع التواصل الإجتماعي وعلاقته بالثقافة الرقمية

(دراسة مسحية لعينة من المستخدمين لبريدي موب)

والمسجل بقسم الإعلام والاتصال وعلم المكتبات،

شعبة علوم الإعلام ولاتصال أقر بأن المذكرة قد استوفت مقتضيات البحث العلمي من حيث الشكل والمضمون ومن ثمة أعطيا لإذن بإيداعها.

إمضاء المشرف


بسم الله الرحمن الرحيم

شكر وعرفان

بسم الله الذي زرع النجاح في كل الدروب و غرس حب العمل في كل القلوب.....

الحمد لله الذي بنعمته تتم الصالحات و الحمد لله الذي منحني الصبر و القدرة على إتمام هذا العمل المتواضع.

أتقدم بجزيل الشكر والعرفان إلى أستاذتي المشرفة "**صونية ڤوراري** "على ما بذلته من جهد في التوجيه و النصح و المتابعة في هذا البحث.

كما أتوجه بشكري الخالص إلى إدارة كلية العلوم الإنسانية و كافة الأساتذة على التسهيلات التي قدمت لي خلال هذا المشوار الجامعي.

كما أتوجه بالشكر إلى الأساتذة الذين تفضلوا بقراءة هذا البحث و مناقشته.

و إلى كل من ساعدني على إنجاز هذا البحث من قريب أو من بعيد و لو بالكلمة الطيبة.

إهـــــــــداء

ما سلكنا البدايات إلا بتسييره و ما بلغنا النهايات إلا بتوفيقه وما حققنا الغايات إلا بفضله فالحمد لله الذي وفقني لتثمين هذه الخطوة في مسيرتي الدراسية

اهدي هذا النجاح إلي نفسي أولا، ثم إلى كل من سعى معي من قريب أو من بعيد لإتمام هذه المسيرة دمتم لي سندا

إلى من الجنة تحت أقدامها إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي صديقتي وحبيبتي أمي غاليتي

إلى من دعمني بلا حدود وأعطاني بلا مقابل إلى من علمني أن دنيا كفاح وسلاحها العلم والمعرفة أبي الغالي

إلى من جاد على بوقته وأكرمني بفضله إقرار منى بصبره وتعبه واعترافا بحقه حيث كان خير عون لى رفيق دربي زوجي

والى من شد الله بهم عضدي إخوتي وأخواتي

إلى قرة عيني ونبض قلبي في حياتي أولادي كنان وركان

إلى من كانا سببا لتسهيل طريقي وإتمام مشواري الدراسي رفيقتي زوجة أخ زوجي نادية

إلى من كانت حريصة على دعمي زوجة أب زوجي زهرة

إلى من كان أبا وسندا وعوضا لابي في بيت عائلة زوجي أبي الثاني مسعود

إلى صديقاتي الذين جعلوا هذه الرحلة أكثر متعة واقل صعوبة، شكرا لكل لحظة ودعم

لكل كلمة مشجعة، و لكل الذكريات الجميلة التي صنعناها معا

وأخيرا من قال انأ لها نالها...

﴿فَإِنَّ مَعَ ٱلۡعُسۡرِ يُسۡرًا ۝٥ إِنَّ مَعَ ٱلۡعُسۡرِ يُسۡرٗا ۝٦﴾ [الشرح ٥-٦]

الملخص

تهدف الدراسة إلى فهم ظاهرة الاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي وعلاقتها بالثقافة الرقمية، وذلك من خلال دراسة ميدانية اعتمدت على المنهج المسحي لعينة متاحة بلغ عدد أفرادها 100 مبحوث من مستخدمي تطبيق بريدي موب في الجزائر. وجاءت هذه الدراسة استجابة لتزايد حالات الاحتيال الإلكتروني التي يتعرض لها الأفراد عبر الفضاءات الرقمية، خاصة في ظل الاستخدام الواسع للتكنولوجيات الحديثة دون امتلاك وعي كافٍ بمخاطرها.

كما تهدف إلى توضيح أبرز الأساليب الاحتيالية وفهم العالقة العكسية بين الاحتيال الإلكتروني والثقافة الرقمية، ودور مواقع التواصل الاجتماعي في تسهيل هذه الجرائم. وكما هدفت إلى تقديم استراتيجيات لتعزيز الثقافة الرقمية وطرق الكشف عن العمليات الاحتيالية وسد الفجوة الرقمية.

الكلمات المفتاحية: الاحتيال الإلكتروني – الثقافة الرقمية – سد الفجوة الرقمية – مواقع التواصل الاجتماعي – بريدي موب – فيسبوك – انستغرام.

Abstract

This study seeks to explore the phenomenon of electronic fraud via social media platforms and its relationship with digital culture. It is based on a field survey that adopted the descriptive survey methodology, relying on an available sample of 100 respondents from users of the Baridi Mob application in Algeria. The research emerges in response to the increasing prevalence of electronic fraud incidents targeting individuals within the digital sphere, particularly in the context of widespread modern technology usage without sufficient digital awareness.

The study further aims to identify the most prominent fraudulent techniques and to analyze the inverse correlation between electronic fraud and digital culture. It also examines the role that social media platforms play in facilitating such criminal activities. Moreover, the research proposes strategic recommendations to enhance digital culture, bridge the digital divide, and develop effective methods for detecting fraudulent operations.

Keywords: Electronic fraud – Digital culture – Bridging the digital divide – Social media – Baridi Mob – Facebook – Instagram.

فهرس المحتويات

قائمة الجداول

المقدمـــــــــــة

مقدمـــــــــة

شهد العالم تطور تكنولوجي سريع مما خلق ثورة رقمية، حيث أصبحت الحياة الرقمية جزءاً لا يتجزأ من واقعنا اليومي، حيث أتاحت هاته التقنيات الحديثة فرصاً غير مسبوقة في مختلف المجالات من بينها مجال التواصل، والتجارة، والتعلم، وتقديم الخدمات. وغيرها من المجالات ومع هذا التحول الرقمي الكبير، فلقد برزت أيضاً مجموعة من التحديات الجديدة التي باتت تهدد أمن المستخدمين وثقتهم في هذا الفضاء الإلكتروني، ومن أبرز هاته التهديدات الالكترونية يأتي في مقدمتها الاحتيال الإلكتروني، الذي يشكل أحد أبرز الجرائم السيبرانية انتشاراً وتعقيداً.

فمع تزايد الاعتماد على هاته المنصات الرقمية، خاصة في مجال القطاع المالي وخدمات الدفع الإلكتروني، فلقد زادت حدة هذه الظاهرة، مما جعلها موضوع يحدث دراسة لمجموعة من الباحثين والمتخصصين إلى دراسة أبعادها وآليات مواجهتها.

فلقد أصبح الاحتيال الإلكتروني ظاهرة عالمية لا تقتصر على دولة أو منطقة دون أخرى، وذلك بسبب انتشار وتنوع المستخدمين في البيئة الرقمية خاصة عبر مواقع التواصل الاجتماعي الذي يعد مكانا جيدا للمحتالين بتنفيذ عملياتهم الإجرامية وكما أن هاته الأساليب الاحتيالية تستهدف الأفراد والمؤسسات عبر وسائل متعددة، ومن ابرز هاته الأساليب نجد التصيد الاحتيالي (Phishing)، والبرمجيات الخبيثة (Malware)، وانتحال الشخصية (Identity Theft)، وغيرها.

حيث تكمن خطورة هذه الجرائم في قدرتها على التطور السريع، واستغلال الثغرات التقنية والقانونية، بل وحتى الاستفادة من نقص الوعي الرقمي لدى بعض المستخدمين ما يجعلها فرصة ذهبية للمحتالين.

وفي هذا السياق، تبرز لدينا ما يسمى بالثقافة الرقمية التي تلعب بدورها كعامل حاسم في الحد من انتشار عمليات الاحتيال الإلكتروني، إذ تشكل وعي المستخدمين ومهاراتهم في التعامل الآمن مع التقنية خط الدفاع الأول ضد هذه التهديدات، وطرق الكشف عليها لعدم الوقوع ضحية لها.

وإذا كان الاحتيال الإلكتروني يشكل تحدياً عالمياً، فإن تأثيره يختلف من مجتمع إلى آخر وذالك يعود على حسب درجة النضج الرقمي، والبنية التحتية التكنولوجية، والإطار القانوني المنظم. وغيرها من العوامل التي قد تأثر عليه .

ففي الجزائر، كما في العديد من الدول النامية، فإن القطاع الرقمي يشهد نمواً ملحوظاً، خاصة بعد انتشار استخدام تطبيقات الخدمات المالية عبر الهاتف المحمول، مثل تطبيق "بريدي موب" التابع لبريد الجزائر، الذي يعمل على توفير مجموعة من الخدمات للمواطنين منها تحويل الأموال، الدفع الإلكتروني، وغيرها من المعاملات المصرفية.

ومع هذا التوسع فلقد ازدادت أيضاً محاولات الاحتيال الإلكتروني التي قد تستهدف مستخدمي هذه التطبيقات، مما يطرح تساؤلات حول مدى وعي المستخدمين بهذه المخاطر، وكيف يمكن للثقافة الرقمية أن تلعب دوراً في تعزيز حمايتهم.

من هنا تأتي أهمية هذه الدراسة، التي تسعى إلى استكشاف العلاقة بين الاحتيال الإلكتروني والثقافة الرقمية، من خلال التركيز على عينة من مستخدمي تطبيق "بريدي موب" في الجزائر.

ولتفصيل أكثر في هذا البحث فلقد اعتمدنا في دراستنا هاته على مجموعة من الخطوات المهمة التي تم تنظيمها بالشكل التالي :

أولا قمنا بتقسيم محاور هاته الدراسة إلى ثلاث فصول الفصل الأول تحت عنوان الإطار المنهجي وتم فيه طرح الإشكالية والسؤال الرئيسي والفصل الثاني تحت عنوان الإطار النظري والذي بدوره ينقسم إلى ثلاث مباحث المبحث الأول تحت عنوان ماهية الاحتيال الالكتروني والمبحث الثاني تحت عنوان ماهية مواقع التواصل الاجتماعي والمبحث الثالث تحت عنوان ماهية الثقافة الرقمية، أما بالنسبة للفصل الأخير تحت عنوان الإطار التطبيقي الذي يحتوي على دراسة ميدانية باستخدام استمارة الكترونية .

الفصل الأول

الإطار المنهجـــي للدراسة

خطـــــــــة الدراســـــــة (الفصل الأول)

أولا: إشكالية الدراسة.

ثانيا: أسباب اختيار الموضوع.

ثالثا: أهداف الدراسة .

رابعا: نوع الدراسة.

خامسا: منهج الدراسة.

سادسا:أدوات جمع بيانات الدراسة.

سابعا: مجتمع الدراسة والعينة .

ثامنا: تحديد مفاهيم الدراسة.

تاسعا: صعوبات الدراسة.

عاشرا: نظرية الدراسة.

إحدى عشر: الدراسات السابقة.

أولا: إشكالية الدراسة

في ظل التحول الرقمي الهائل والمتسارع الذي يشهده العالم يوميًا، ومع التطور التكنولوجي المستمر، برزت أشكال جديدة من التهديدات السيبرانية التي أصبحت تشكل خطرًا كبيرًا على المستخدمين الذين يتعاملون مع الإنترنت بشكل يومي ودائم. فقد غدا الإنترنت بمثابة الوريد الذي يضخ الدم إلى القلب؛ فإذا توقف، توقفت معه الحياة بكل جوانبها.

وأمام هذا الاعتماد الكبير على الإنترنت في مختلف مناحي الحياة، نشأ ما يُعرف بـ"المجتمع الرقمي" أو "الجمهور الرقمي"، نتيجة للعدد الهائل من المستخدمين، حيث بلغت نسبة مستخدمي الإنترنت في العالم نحو 68٪ من سكان العالم، وذلك وفقًا لآخر دراسة أُجريت سنة 2024.

وقد أدى هذا الانتشار الواسع إلى بروز العديد من الجرائم والتهديدات الإلكترونية، ومن أخطرها جريمة الاحتيال الإلكتروني، التي باتت تُهدد الأفراد، والمؤسسات، وحتى الدول. وتزايدت خطورتها مع ظهور مواقع التواصل الاجتماعي مثل فيسبوك، إنستغرام، وتطبيقات المواعدة والدردشة، والتي تُعد من أكثر البيئات التي تُسجل فيها شكاوى تتعلق بالاحتيال والتهديدات الإلكترونية.

ومع هذا التزايد المستمر في استخدام وسائل التواصل الاجتماعي، أصبحت هذه المنصات بيئة خصبة للمحتالين بسبب الكم الهائل من المستخدمين، مما ساهم في انتشار عمليات الاحتيال الإلكتروني بمختلف أشكالها.

وتُعد ظاهرة الاحتيال الإلكتروني من أبرز التحديات التي تواجه الأفراد والمجتمعات في العصر الرقمي، نظرًا لاعتماد الناس المتزايد على الإنترنت في التسوق الإلكتروني، والمعاملات المصرفية، والمراسلات الشخصية.

وتكمن خطورة الاحتيال الإلكتروني في استخدام التكنولوجيا لارتكاب جرائم مثل سرقة المعلومات الشخصية، والاحتيال المالي، واستخدام البرمجيات الخبيثة، حيث تتسم هذه الجرائم بسهولة ارتكابها وسرعة انتشارها عبر الدول والقارات.

ومن أبرز الأمثلة المحلية على هذا الخطر، نجد الاستخدام العشوائي لتطبيق "بريدي موب" دون الإلمام بتفاصيله وآليات الأمان الخاصة به، مما يجعل مستخدميه عرضة للوقوع في فخ الاحتيال الإلكتروني.

ويُعد هذا التطبيق أداة رئيسية للمعاملات المالية الإلكترونية في الجزائر، ولكنه أيضًا هدف للمحتالين، مما يُبرز أهمية رفع مستوى الثقافة الرقمية كوسيلة فعّالة لمواجهة هذا التهديد.

وقد بدأ مفهوم "الثقافة الرقمية" بالظهور في تسعينيات القرن الماضي بالتزامن مع توسّع استخدام الإنترنت والحواسيب، إلا أنه بدأ يلقى رواجًا حقيقيًا مع العقد الأول من الألفية الثالثة، خصوصًا بعد ظهور الهواتف الذكية وتحول جزء كبير من التفاعل الإنساني إلى الفضاء الرقمي.

وبالرغم من تزايد الوعي بالمخاطر الرقمية، وتنظيم حملات تحسيسية للتصدي لها، إلا أن ظاهرة الاحتيال الإلكتروني لا تزال في تزايد مستمر، نتيجة التطور التقني المتسارع، وغياب التوعية الكافية بثقافة الاستخدام الرقمي الآمن.

ومن هنا، يتبلور التساؤل الرئيسي لهذه الدراسة:

كيف تؤثر الثقافة الرقمية على تجنب الاحتيال الإلكتروني ؟

وقد تفرع من هذا التساؤل مجموعة من الأسئلة الفرعية جاءت كالتالي:

- ما هي أبرز أساليب وخصائص الاحتيال الإلكتروني التي يتعرض لها مستخدمو تطبيق بريدي موب عبر مواقع التواصل الاجتماعي؟
- ما مدى امتلاك مستخدمي تطبيق بريدي موب لمهارات الثقافة الرقمية التي تساعدهم في الوقاية من الاحتيال الإلكتروني؟
- كيف تساهم الثقافة الرقمية في الحد من الوقوع ضحية للاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي؟

ثانيا: أسباب اختيار الموضوع

ترجع أسباب اختيار موضوع الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي وعلاقته بالتوعية الثقافية الالكترونية إلى أسباب ذاتية وأخرى موضوعية تشكل في مجملها حافزا أساسيا لتقصي أبعاد هذا الموضوع .

1. **أسباب ذاتية:**

- وقوعي ضحية في عملية احتيال الكتروني عبر منصة فيسبوك.
- اهتمامي بالمواضيع التكنولوجية الحديثة .
- الرغبة في دراسة هذا الموضوع بشكل عميق كونه موضوع حديث وعميق.
- الرغبة في زيادة كفاءتي في البحث العلمي مما يأهلني للحصول على شهادة الماستر في الإعلام والاتصال تخصص سمعي البصري.

2. **أسباب موضوعية:**

- معرفة الأسباب التي أدت إلى غياب الوعي الثقافي.
- كشف بعض الطرق المستعملة في الاحتيال بواسطة مواقع التواصل الاجتماعي .
- طرق تجنب وكشف أساليب الاحتيال الشائعة .
- كيفية نشر التوعية الثقافية الالكترونية.

ثالثا: أهداف الدراسة

تهدف هذه الدراسة إلى ما يلي:

- رصد وتحليل الأساليب المتنوعة للاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي، خاصة في تعاملات مستخدمي تطبيق بريدي موب.
- قياس مستوى الثقافة الرقمية لدى عينة من مستخدمي تطبيق بريدي موب، وتحديد درجة وعيهم بمخاطر الفضاء الرقمي.
- تحليل العلاقة بين مستوى الثقافة الرقمية ومخاطر الاحتيال الإلكتروني، والكشف عن دور التوعية الرقمية في الوقاية.

- اقتراح استراتيجيات لتعزيز الثقافة الرقمية كوسيلة للحد من انتشار جرائم الاحتيال عبر التطبيقات الرقمية ومواقع التواصل.
- فهم العلاقة العكسية بين الاحتيال الالكتروني والثقافة الرقمية.

رابعا: نوع الدراسة

نوع الدراسة وصفية استكشافية تهدف إلى فهم الظاهرة موضوع البحث بشكل عميق ووصف خصائصها والعوامل المؤثرة فيها دون السعي إلى إثبات علاقة سببية مباشرة فيما يلي تصور شامل لتنفيذ دراسة وصفية استكشافية لموضوع الاحتيال الالكتروني وعلاقته بالثقافة الرقمية.

خامسا: منهج الدراسة

يُعرّف المنهج بشكل عام بأنه الطريقة المتبعة للكشف عن الحقائق، والتي تخضع لمجموعة من القواعد العامة المتعلقة بجمع البيانات وتحليلها، مما يساهم في الوصول إلى نتائج ملموسة من خلال الاستنباط والاستقراء. **(راضي م.، 2012، صفحة 118)**

في هذه الدراسة، تم استخدام المنهج المسحي بجزأيه الوصفي والتحليلي، نظراً لأن البحث يركز على جمع البيانات والمعلومات المتعلقة بالظاهرة المدروسة وتفسيرها. فالمنهج المسحي هو عملية منظمة لتجميع البيانات المتعلقة بمؤسسات إدارية أو علمية أو ثقافية خلال فترة زمنية محددة، بهدف تحليلها ووصفها. وهو بمثابة محاولة بحثية منظمة لتقييم وضع معين أو نظام أو جماعة، للوصول إلى معلومات واضحة ودقيقة حول ظاهرة أو موضوع معين.

تجدر الإشارة إلى أن المفاهيم المرتبطة بالمنهج المسحي في الدراسات العلمية تتفق على أنه يركز على دراسة الظواهر أو الموضوعات القائمة في جماعة معينة خلال فترة زمنية محددة ومكان معين، أي وقت إجراء البحث. (عادل، 2014، صفحة 60)

كما قمت بنشر الاستمارة الالكترونية لجمع البيانات والاجابة على الأأسئلة على صفحتي فيسبوك باسم Sabrin Nekhalوذالك لأنها صفحة تجارية خاصة ببيع المستلزمات المنزلية وغيرها من المنتجات وعليه فكانت مناسبة جدا لطرح الاستمارة فيها.

سادسا : أدوات الدراسة

1. الإستبيان:

الاستبيان هو أحد وسائل البحث العلمية المستعملة من طرف الباحث لجمع معلومات من أشخاص في شكل استمارة تضم أسئلة، لاستنباط حقائق معينة تتعلق بإشكالية محددة ترسل أو تسلم إلى الأشخاص الذين تم اختيارهم لموضوع الدراسة ليقوموا بتسجيل إجاباتهم عن الأسئلة وإعادتها للباحث هو تصميم فني لمجموعة من الأسئلة حول موضوع معين لتمكين الباحث من الحصول على البيانات اللازمة للبحث من خلال إجابة الأشخاص المعنيين وهي أكثر توفيرا للجهد، الوقت والمال، نلجأ للاستبيان عندما تتطلب الدراسة تقديرات كمية لظاهرة ما استخراج مؤشرات أو إجراء مقارنات..) وهي ملائمة أكثر في البحوث الميدانية عندما يكون المجتمع كبير والظاهرة المدروسة منتشرة والمعلومات المراد جمعها كثيرة وغير متوفرة. (سعاد، صفحة 03)

2. الأساليب الإحصائية المستخدمة:

تم الحصول على البيانات الأولية من خلال تصميم إستبانة وتوزيعها على عينة من مجتمع الدراسة، ومن ثم تفريغها وتحليلها باستخدام برنامج (Statistical package for Social Science)Spss V.20 وباستخدام الاختبارات الإحصائية المناسبة بهدف الوصول إلى دلالات ذات قيمة ومؤشرات تدعم موضوع البحث.

وللإجابة على أسئلة البحث، تم استخدام أساليب الإحصاء الوصفي وذلك باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (Spss.V20) والذي يتكون من:

- مقاييس الإحصاء الوصفي (Descriptive StatisticMeasures): وذلك لوصف مجتمع البحث وإظهار خصائصه، بالاعتماد على النسب المئوية والتكرارات.
- معامل الثبات ألفا كرونباخ (Cronbach's Coefficient Alpha): وذلك لقياس ثبات أداة البحث.
- معامل صدق المحك: وذلك لقياس صدق أداة البحث.

سابعا: مجتمع البحث والعينة

1. مجتمع البحث

يعتبر مجتمع الدراسة جميع الحالات والافراد والأشياء التي يتجه الباحث لدراستها. (العزاوي، 2008، صفحة 180)

ومجتمع الدراسة لموضوع بحثنا هو مستخدمي تطبيق بريدي في التعاملات الشرائية عبر المواقع الاجتماعية لتسديد الفواتير والمنتوجات وغيرها من العمليات المالية، أي دراستنا ستقوم على المتعاملين مع بريدي موب أي الذين يستخدمون تطبيق بريدي موب بشكل دوري لإجراء معاملاتهن المالية.

وكما سنقوم بدراسة مجموعة تكون قد تعرضت او تأثرت بالاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي: حيث يشكل هذا المجتمع المستهدف الأساسي للدراسة، المجال الجغرافي: الأشخاص المتعاملين مع تطبيق بريدي موب داخل الولاية بسكرة .

2. عينة البحث

تُعد العينة جزءاً من مجتمع البحث، حيث يقوم الباحث باختيارها بطرق متنوعة لتمثيل المجتمع الأصلي. تهدف العينة إلى تحقيق أهداف الدراسة بكفاءة، مما يوفر الوقت والجهد مقارنة بدراسة المجتمع بأكمله. كما يجب أن تكون العينة ممثلة تمثيلاً دقيقاً وعادلاً للمجتمع الأصلي، بحيث يمكن تعميم نتائج الدراسة عليه. (المشهداني، 2019 ، صفحة 85)

وتُعرَّف العينة أيضاً بأنها مجموعة من الوحدات المستمدة من المجتمع الإحصائي، والتي تحمل نفس مواصفات ذلك المجتمع. يتم اختيارها وفق معايير محددة لضمان تمثيلها الصحيح للمجتمع الأصلي. (مجلة تنوير للبحوث الانسانية والاجتماعية، الصفحات 264-265)

العينة هي جزء من المجتمع يتم دراسته لجمع معلومات موثوقة يمكن تعميم نتائجها على المجتمع الأصلي. يستخدم الباحث العينة للحصول على نتائج دقيقة وسريعة، كما أنها تُسهّل دراسة المجتمع في حالات صعوبة أو استحالة الوصول إليه بالكامل.

هناك أنواع متعددة من العينات يختارها الباحث بناءً على طبيعة الدراسة، مما يتيح تعميم النتائج على المجتمع الأصلي. في هذه الدراسة، اعتمدنا على:

1. العينة العرضية :

يشمل هذا النوع العديد من طرق اختيار العينة مثل مقابلة من يتصادف وجودهم في الشارع وهي طريقة تتبعها القنوات التلفزيونية للحصول على قراءة لاتجاهات الرأي العام. (الجبار)

في العديد من المواقف يتم اختيار العينة من مجموعات من المتطوعين، المشكلة في هذا النوع من طرق اختيار العينة أن ليس هنالك دليل يؤكد أنها ممثلة للمجتمع الذي تود التعميم عنه في دراستنا، التي تهدف إلى فهم العلاقة بين الاحتيال الالكتروني والثقافة الرقمية ومدى وعي الأفراد المستخدمين لتطبيق بريدي موب بطرق الأمان لعدم وقوعهم ضحية الاحتيال الالكتروني ومعرفة إذا كان لديهم ثقة في إجراء معاملاتهم المالية عبر تطبيق بريدي موب. لذلك، اعتمدت على العينة العرضية، حيث بلغ عدد الردود 100 شخص .

ولقد تم اختيار وتحديد هذا النوع من العينة بعد مراجعات وإطلاع وفق اعتبارات منهجية أهمها:

- مناسبة هذا النوع من العينة لمنهج الدراسة الحالي والذي يعتمد في الأساس على معلومات كمية تكون مفيدة أكثر لتكامل عناصر البحث وتسلسلها في قالب موضوعي ضمن التخصص الذي يندرج تحته هذا البحث.
- سهولة الاختيار الكمي للبيانات التي يوفر تحليلها إجابة على تساؤلات الدراسة. الخصائص غير الانتقائية التي يوفرها هذا النوع من العينات الاحتمالية للباحث بهدف جمع معلومات بها كل خصائص مجتمع الدراسة يكون له جدوى في موضوع الدراسة دون الشك في النتائج وتضييع الجهد والوقت نظرا لمحدودية الوقت والجهد للتقصي حول البحث الحالي.
- تناسب الدراسات التوكيدية في مضمونها .

2. صدق وثبات العينة

اختبار صدق وثبات أداة الدراسة

أ. صدق أداة البحث (Validity)

يقصد بصدق الأداة قدرة الإستبانة على قياس المتغيرات التي صممت لقياسها، وللتحقق من صدق الإستبانة المستخدمة في البحث نعتمد على ما يلي:

- **صدق المحتوى أو الصدق الظاهري:**

تم عرض الاستبانة المعتمدة في الدراسة على عدد من الأساتذة المحكمين وذلك للحكم على نسبة العبارات لموضوع الدراسة وسلامة الصياغة اللغوية للعبارات، من أجل تصحيحها وإعطاء حكم ظاهري عن مدى ملائمة عبارات الاستبانة لموضوع البحث، وقد تم الأخذ بعين الاعتبار ملاحظات الأساتذة المحكمين وقمنا بإجراء التعديلات المطلوبة. وقد تم تحكيم هذه الاستمارة من قبل أساتذة التخصص إعلام واتصال بسكرة جامعة محمد خيضر بسكرة.

- نجاة علمي رتبة أستاذة محاضرة أ.
- شيقر سليمة رتبة أستاذة محاضرة ب .
- نهلة حفيظي رتبة أستاذة محاضرة أ.

- **صدق المحك:**

يتم حساب معامل "صدق المحك" من خلال أخذ الجذر التربيعي لمعامل الثبات" ألفا كرونباخ"، وذلك كما هو موضح في الجدول الموالي، إذ نجد أن معامل الصدق الكلي لأداة البحث بلغ (0.875) وهو معامل مرتفع ومناسب لأغراض وأهداف هذا البحث. وبهذا يمكننا القول إن جميع عبارات أداة البحث هي صادقة لما وضعت لقياسه.

ب. ثبات الأداة (Reliability)

ويقصد بها مدى الحصول على نفس النتائج أو نتائج متقاربة لو كرر البحث في ظروف متشابهة باستخدام الأداة نفسها. وفي هذا البحث تم قياس ثبات أداة البحث باستخدام معامل الثبات ألفا كرونباخ الذي يحدد مستوى قبول أداة القياس بمستوى (0.70) فأكثر، حيث كانت النتائج كما هي موضحة في الجدول الموالي:

الجدول 1: اختبار معامل الصدق والثبات للاستبيان

المحور	عدد عبارات القياس	معامل الثبات Alpha de Cronbach	معامل الصدق
الاستبيان ككل	18	0.767	0.875

المصدر: من إعداد الطالبة بالاعتماد على نتائج SPSS

من خلال الجدول السابق يتبيّن أنّ معامل ثبات الاتساق الداخلي"ألفا كرونباخ" للاستبانة بلغت(0.767) وهي قيمة مرتفعة، ما يدل على أنّ الاستمارة ثابتة أي أنّها تعطي نفس النتائج إذا تمّ استخدامها أو إعادتها مرّة أخرى تحت ظروف مماثلة.

ثامنا: تحديد المفاهيم

لتحديد مفاهيم الدراسة الخاصة بموضوع "الاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي وعلاقته بالتوعية الثقافية الإلكترونية: دراسة مسحية لعينة من المتعاملين مع بريدي موب"، يمكن صياغة المفاهيم وفقًا للعناصر الرئيسية التالية مع الإشارة إلى مراجع تساعد في تفسيرها:

1. الاحتيال الالكتروني

التعريف الإجرائي:

للاحتيال الالكتروني هو احدث الجرائم الالكترونية الحديثة التي تتم عن طريق مجموعة من التقنيات والمهارات الغير مشروعة ويتم كل هذا بواسطة الاستعانة بشبكة الانترنت التي تسهل عملية ارتكاب هاته الجرائم الالكترونية .

وهذا ما يترتب عليه مجموعة من الأضرار منها المادية ومنها المعنوية على الشخص الضحية في تلك العملية وقد يهدف القائم بالعملية علي مجموعة من الأمور التي يبحث عنها منها اختراق لبيانات شخصية أو سرقة أموال وغيرها من الأهداف التي تدفعهم للقيام بمثل هاته العمليات الاحتيالية.

2. مواقع التواصل الاجتماعي

التعريف الإجرائي:

مواقع التواصل الاجتماعي هي منصات إلكترونية تفاعلية تستخدم عبر الإنترنت تمكن الأفراد والجماعات من إنشاء محتوى ومشاركته والتفاعل مع الآخرين من خلال نصوص وصور ومقاطع فيديو ورسائل صوتية تشمل هذه المواقع تطبيقات مثل: فيسبوك، تويتر، انستغرام، تيك توك وتقاس درجة استخدامها بعدد ساعات التصفح و مستوى التفاعل والتعليقات والإعجابات وعدد الأصدقاء والمتابعين.

3. الثقافة الرقمية

التعريف الإجرائي:

الثقافة الرقمية هي مجموعة من الأنشطة والعمليات التي تهدف إلى نشر المعرفة وتعزيز الوعي بالقيم والعادات والمفاهيم الثقافية باستخدام الوسائل والتقنيات الرقمية مثل: المواقع الإلكترونية وسائل التواصل الاجتماعي التطبيقات الذكية والمدونات تقاس فعالية هذه التوعية من خلال مستوى وصول المحتوى للجمهور درجة تفاعلهم معه ومدى تأثيره في تعديل أو تعزيز سلوكياتهم واتجاهاتهم الثقافية.

4. بريدي موب

التعريف الاجرائي:

هو تطبيق مالي إلكتروني مقدم من مؤسسة بريد الجزائر يهدف إلى تسهيل المعاملات المالية مثل الدفع الإلكتروني وتحويل الأموال.

تطبيق بريدي موب هو تطبيق مصرفي مخصص لتسهيل العمليات المالية والإدارية المتعلقة بالخدمات البريدية والمصرفية يستخدم هذا التطبيق بشكل واسع في بعض الدول مثل: الجزائر من خلال مؤسسة بريد الجزائر حيث يتيح للعملاء إدارة حساباتهم البريدية حسابات سيسبي عبر هواتفهم الذكية بطريقة سهلة وآمنة.

تاسعا : صعوبات الدراسة

- من ابرز الصعوبات التي واجهتني في هذه الدراسة هي قلة المراجع حول الثقافة الرقمية خصوصا المراجع العربية لانه مصطلح جديدا نوعا ما .
- وكذالك قلة وجود مصادر تتكلم عن العلاقة العكسية بين الاحتيال الالكتروني والثقافة الرقمية.
- صعوبة تنزيل وتحميل المراجع الأجنبية لأن معظمها تكون مدفوعة بالعملة الصعبة.

عاشرا: نظرية الدراسة

1. الفجوة الرقمية:

خلال التسعينات من القرن الماضي بدأ الباحثون وصانعو السياسات مناقشة وجود ما يسمى ب"الفجوة الرقمية "وهي تمييز بين الاشخاص الذين لديهم إمكانية الوصول الى تكنولوجيا الاعلام والاتصال والذين لا يستطيعون ذالك. (Door Alexander van Deursen en Jan van Dijk , The Dijital divide،, An introduction University of Twente, utwente.nlut)

ومن ابرز الباحثين الذين قاموا بتعريف الفجوة الرقمية نجد بيكر .Baker حيث عرفها بأنها "بالنسبة للمستخدم أو المنتج بأنها الوضعية القصوى من منظور الربط أو الوصول إلى التكنولوجيا وتوفير المضامين والخدمات والجدو ى أو الوعي المرتبط بالقيمة الحقيقية من منظور المستخدمين، بالنسبة لاستخدام تكنولوجيات المعلومات والاتصالات والخدمات المرتبطة بها. (مستخدم،فجوة الرقمية، 2025)

ويعرفها الاتحاد الدولي للاتصالات "بأنها " الاختلاف بين من يملك ومن لا يملك فرص النفاد أو الوصول إلى المعلومات عبر وسائل وتقنيات الاتصال الهاتف الثابت والمحمول والحاسوب والانترنت وخدمة الحزم (العريضة وقد تكون الفجوة بين البلدان المتقدمة والنامية أو بين البلدان ضمن المجموعة الواحدة أو في البلد الواحد أي بين الريف والمدينة أو بين السكان بحسب خصائص العمر والجنس والدخل والعرق. (ITU، 2010، صفحة 40)

ولقد عرف جيمس الفجوة الرقمية بأنها" التوزيع غير المتكافئ للحواسيب ووصلات الانترنت وآلات الفاكس وما الى ذلك بين البلدان"، بينما يرى نوريس بأنها تتشكل من 3 أبعاد، فهي تفهم " كظاهرة متعددة الابعاد تشمل ثلاثة جوانب مميزة، فالفجوة العالمية تشير الى الاختلاف في النفاذ الى الانترنت بين المجتمعات الصناعية والمجتمعات النامية، والفجوة الاجتماعية هي الفجوة بين مصادر المعلومات بين الاغنياء والفقراء في كل أمة. (مستخدم،فجوة الرقمية، 2025)

2. محتوي الفجوة الرقمية

الفجوة الرقمية تعتبر الفجوة هي الام التي تحوي في طياتها العديد من الفجوات وقد تنقسم هذه الفجوات إلى (القادر و رمضاني، صفحة 218) :

- فجوة تكنولوجية اي هو فجوة كبيرة بين التقدم التكنولوجي للدول المتقدمة والدول النامية.
- فجوة معرفية اي فارق في تحصيل المعلومات وانتقالها بين الدول المتقدمة والدول النامية.
- جوة في التعليم أي فارق كبير في التعليم وأساليبه وطرق وأنشطة البحث العلمي والتطور بين الدول المتقدمة والدول النامية.
- فجوة في الحريات و الديمقراطية يعني فجوة كبيرة بين حرية التعبير وحرية الرأي والمشاركة في صنع القرار بين الدول المتقدمة والدول النامية.

3. أسباب الفجوة الرقمية

وهناك مجموعة من الأسباب أدت إلى ظهور الفجوة الرقمي ومن أبرزها نذكر :

أ. الأسباب التكنولوجية وقد تم تفريعها إلى الأسباب التالية:

- سرعة التطور التكنولوجي.
- تنامي الاحتكار التكنولوجي.
- شدة الاندماج المعرفي.
- تفاقم الانغلاق التكنولوجي.

ب. الأسباب الاقتصادية من أهمها:

- ارتفاع كلفة توطين تكنولوجيا المعلومات.
- تكتل الكبار على الصغار.
- التهام الشركات المتعددة الجنسية للأسواق المحلية.
- كلفة الملكية الفكرية.
- انحياز التكنولوجيا اقتصاديا إلى صف القوى على حساب الضعيف.

ت. الأسباب السياسية ومن أبرزها

- صعوبة وضع سياسات التنمية المعلوماتية.
- سيطرة الولايات المتحدة عالميا على المحيط الجي ومعلوماتي.
- سيطرة حكومات الدول النامية على الوضع المعلوماتي محليا.
- انحياز المنظمات الدولية إلى صف الكبار.

ث. الأسباب الاجتماعية: ومن أبرزها:

- تدني التعليم وعدم توافر فرص التعلم.
- الأمية أغلبهم نساء.
- الجمود المجتمعي.
- الجمود التنظيمي والتشريعي.
- غياب الثقافة العلمية التكنولوجية.

وهذه الأسباب مجتمعة ثم شرحها في كتاب الفجوة الرقمية نبيل على ونادية حجازي وقد تم ذكر أسباب إضافية وهي خاصة بمنطقة جغرافية محددة وهي البلدان العربية وهي:

العامل الأول: الصراع الغربي الإسرائيلي الذي يستنزف الموارد العربية ويقف حجرة عشرة أمام إكمال تكتل معلوماتي وثقافي عربي، وقد جاءت أحداث الحادي عشر سبتمبر وتوابعها لتزيد الموقف سواء بما تمارسه الولايات المتحدة من ضغوط على الدول العربية في إطار استراتيجية مكافحة الإرهاب.

العامل الثاني: عدم وقوع الإقليم العربي في مجال أحد المراكز العالمية لتكنولوجيا المعلوماتية. (علي و نادية، 2005، صفحة 26)

إحدى عشر: الدراسات السابقة

1. **جريمة الاحتيال عبر شبكة المعلومات الدولية، الدكتور وائل محمد نصيرات، ودكتورة غادة عبد الرحمن الطريف، دراسة مقارنة النظام السعودي والقانون الاردني.**

أ. **الإشكالية** : ما هي جريمة الاحتيال عبر شبكة المعلومات الدولية ؟

ب. **الأسئلة الفرعية:**

- ما مفهوم جريمة الاحتيال عبر شبكة المعلومات الدولية ؟
- ما أركان جريمة الاحتيال عبر شبكة المعلومات الدولية ؟
- ما أساليب ووسائل التلاعب في البيانات والبرامج الإلكترونية بأشكالها المختلفة ؟
- ما هي تجربة المملكة العربية السعودية والمملكة الأردنية في مكافحة جريمة الاحتيال عبر شبكة المعلومات ؟

ت. **المنهج المستخدم:** تعد هذه الدراسة من الدراسات المكتبية التي تعتمد منهجيا على تحليل وتفسير الأنظمة والنصوص القانونية ذات الصلة بالموضوع.

ث. أوجه الاستفادة :

- التعرف على اهم وسائل القيام بعمليات الاحتيال الالكتروني .
- معرفة النظام السعودي الخاص بهاته الجريمة وهي الاحتيال مع مقارنته بالقانون الاردني.
- التعرف على اركان جريمة الاحتيال عبر شبكة المعلومات الدولية

ج. **أوجه التشابه :**

- تعريف بالاحتيال بواسطة استعمال شبكة المعلومات الدولية.
- طرق ارتكاب الاحتيال وتأثيراته.

ح. **أوجه الاختلاف :**

- دراستي تقوم على فهم الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي عكس الدراسة فهي تقوم على الاحتيال بصفة عامة عبر شبكة الانترنت في مختلف البرامج والتطبيقات

2. **متطلبات نشر الثقافة الرقمية بالجامعات المصرية من وجهة نظر أعضاء هيئة التدريس، أ.م. د/ محمد السيد فرج الماظ . دراسة تحليلية .**

أ. **الإشكالية:** ما متطلبات نشر الثقافة الرقمية بالجامعات المصرية من وجهة نظر أعضاء هيئة التدريس ؟

ب. **الأسئلة الفرعية :**

- ما الاطار المفاهيمي للثقافة الرقمية ؟
- ما أهم الاتجاهات الحديثة لنشر الثقافة الرقمية لدى طلاب الجامعات ؟
- ما واقع الثقافة الرقمية بالجامعات المصرية طبقا للواقع الميداني ؟
- ما التصور المقترح لنشر الثقافة الرقمية بالجامعات المصرية ؟

ت. **المنهج المستخدم** : تم استخدام المنهج الوصفي لدراسة وتحليل الثقافة الرقمية بالجامعات المصرية بأبعادها المختلفة.

ث. **أوجه الاستفادة :**

- التعرف علي المفاهيم المختلفة لثقافة الرقمية وتزويدي بها.
- التعرف علي اهم طرق نسر الثقافة الرقمية.
- التعرف على ابعاد الثقافة الرقمية المختلفة.

ج. **أوجه التشابه :**

- التعرف على مفهوم الثقافة الرقمية .
- أهم طرق نشر الثقافة الرقمية.
- تأثير الثقافة الرقمية على الأفراد والمستخدمين.

ح. أوجه الاختلاف:

- دراستي تهدف الي معرفة العلاقة بين الثقافة الرقمية والاحتيال الالكتروني عكس إن هاته الدراسة تدرس متطلبات نشر الثقافة الرقمية بالجامعات المصرية ودراسة أبعادها المختلفة.
- دراستي تهدف إلى فهم خصائص الثقافة الرقمية ومدى أهمية الثقافة الرقمية.

الفصل الثانـــــي

الإطار النظري للدراسة

خطـــــــــة الدراســـــــة(الفصل الثاني)

المبحث الأول: الاحتيال الالكتروني

أولا: تعريف الاحتيال الالكتروني.

ثانيا: أنواع وأساليب الاحتيال الإلكتروني.

ثالثا: أسباب الاحتيال الالكتروني وطرق الحماية منه.

رابعا: أشهر طرق الاحتيال عبر تطبيق بريدي موب .

المبحث الثاني: مواقع التواصل الاجتماعي

أولا: تعريف مواقع التواصل الاجتماعي.

ثانيا: دورها في انتشار الاحتيال.

ثالثا: أشهر المنصات التي يتم عليها الإحتيال.

رابعا: طرق الحماية من الاحتيال عبر المواقع.

المبحث الثالث: الثقافة الرقمية

أولا: تعريف الثقافة الرقمية.

ثانيا: أهمية نشر الثقافة الرقمية وخصائصها.

ثالثا:أهم طرق نشر واكتساب الثقافة الرقمية.

رابعا: العلاقة بين الثقافة الرقمية والاحتيال الالكتروني.

المبحث الأول: الاحتيال الالكتروني

سبب تزايد التطورات التقنية في مجال التكنولوجيا ابدأ إلى ظهور مجموعة من المشاكل والجرائم من بينها الاحتيال الإلكتروني حيث تساعد هذه التطورات المحتالين على تنفيذي جرائمهم من خلال التلاعب في البيانات والبرامج الإلكترونية.

أولا: تعريف الاحتيال الالكتروني

1. الاحتيال الالكتروني:

لغة: الاحتيال هو الحذق وجودة النظر القدرة على دقة التصرف الاحتيال والمحاولة مطالبتك الشيء بالحيل والحيلة هي المكر والخديعة ولكي تري كل فعل يقصد فعله به خلاف ما يقتضيه ظاهره.

اصطلاحا: هو الاستيلاء علي مال مملوك للغير بخداعه وحمله على تسليم ذالك المال وعرف بأنه استعمال الجاني وسيلة من وسائل التدليس المحددة علي سبيل الحصر. (صالح عبد الفتاح، 2008، الصفحات 8-9)

اختلف الفقهاء في الوصول إلى تعريف محدد لجريمة الاحتيال الإلكتروني الاختلاف فيهم في الزاوية التي ينظر إليها منه ومن تعريفاته الاستلام حية نتناول على سبيل المثال:

جريمة الاحتيال هي الاستيلاء على الحيز الكاملة الإيميل الغير بوسيلة يشوبها الخداع تسفر عن تسليمي ذلك الميل وعرفها آخر بأنها استعمال وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني ميل مملوكا لغيره نتيجة الوقوع في الغلط. (شهيرة و سويح، 2019)

الاحتيال الإلكتروني يعتبر إحدى الطرق الحديثة المتطورة التي يتم اللجوء إليها الوصول واختراق أهداف معينة بطرق غير مشروعة استنادا إلى وجود شبكة الإنترنت دون النظر إلى الأضرار المعنوية أو المادية التي تترتب على التعدي على أجهزة وخصوصيات الآخرين ويكون الفاعل في هذا النوع من الجرائم شخص ذو مهارات تقنية عالية قادرا على استخدام خبراته في اختراق البيانات السرية بغية الحصول على معلومات واتصالات مجانية. (على، موفق، و آخرون، صفحة 336)

الاعتماد على الحاسب الآلي وتتوافر في الشبكة العنكبوتية التي تعد جوهر الجريمة الاحتيال الإلكتروني إذ وبدونها لا يكون هناك وجود للاحتيال الإلكتروني وارتبط تعريفها بالمفهوم العام للجريمة الإلكترونية التي يدخل الاحتيال في احدي أساليبها الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي وهذا ما أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم. (الكعبي، 2009، صفحة 32)

وكذلك عرفت بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي.

وكما عرف بأنه كل خطر ينشأ عن استخدام المحتالين للبريد الإلكتروني أو المواقع الإلكترونية أو البرمجيات الخبيثة .أو غيرها من الأدوات، للحصول على المعلومات الشخصية للمستخدم أو خداعه لتقديم معلوماته الشخصية وذالك لاستثمارها لتحقيق غايات عديدة ومنها غايات مالية غير مشروعة. (هيئة الحكومة الرقمية,، 2023)

ثانيا: أنواع وأساليب الاحتيال الإلكتروني

1. أنواع الاحتيال الإلكتروني:

أ. احتيال الهوية أو انتحال الشخصية

وهو احد أشهر أنواع الاحتيال الالكتروني، يتم عن طريق سرقة معلومات الأشخاص والدخول إلى الأنظمة بأسمائهم من جل الحصول على منافع مختلفة. (شهيرة و سويح، 2019، صفحة 40)

الاحتيال من خلال استخدام هوية وهمية أو مسروقة في تنفيذ عمل غير نظامي بهدف الحصول على سلع أو خدمات بطريقة غير نظامية. مثل: يشكل استغلال بيانات الهوية الشخصية خطرا كبيرا خصوصا مع الأفراد فتستغل في تنفيذ محاولات احتيال غير مشروعة مثل الاحتيال المالي أو الاستفادة من الخدمات الإجتماعية والخدمات الحكومية أو تشكل تهديدا سياسيا عليهم عند استخدام بياناتهم في محاولات إجرامية دولية . (2023، صفحة 12)

ب. الاحتيال الودي

يتم الاحتيال الودي عن طريق الأسلوب الهادئ واللطيف في التعامل مع الأشخاص وذالك لكسب ثقتهم وتودد لهم بهدف تحقيق غايات سيئة تهدف إلى الإضرار بالأشخاص أو الضحية. (مدخنة، 2024)

وهناك عدة أسباب لوقوع مثل هذا الاحتيال:

- **النسيان:** يعتبر النسيان أحد الأسباب الأكثر شيوعاً للاحتيال الودي. فقد ينسى العميل عملية شراء قام بها، أو يفشل في التعرف الى الرسوم في كشف حساب بطاقة الائتمان الخاصة به. في هذه الحالات، قد يعترض العميل على الرسوم، على الرغم من أنه أجرى عملية الشراء بنفسه. (ماهو الاحتيال الودي)
- **سوء الفهم:** يعد سوء الفهم سبباً شائعاً آخر لهذا النوع من الاحتيال. فقد يسيء العميل فهم شروط وأحكام البيع، أو لا يعي تماماً سياسة الإلغاء أو الإرجاع. وهذا ما قد يُفضي إلى نزاعات لاسترداد المبالغ المدفوعة. (مدخنة، 2024)
- **الشراء الاندفاعي:** يؤدي الشراء الاندفاعي أحياناً إلى الاحتيال الودي. فقد يجري بعض العملاء عملية شراء بناءً على نزوة، ثم يندمون لاحقاً عليها، أو يغيرون رأيهم بشأن المنتج أو الخدمة. (ماهو الاحتيال الودي)

ت. الإحتيال المالي

الاحتيال أو السرقة بهدف سرقة المال، أو تحويله إلى حساب المحتال، أو كلاهما.

مثال: استغلال البيانات الشخصية المالية أو بيانات المؤسسات المالية مثل بيانات المحافظ الاستثمارية أو القوائم المالية والميزانيات بهدف استغلال الثغرات المالية وتحقيق مكاسب غير مشروعة. (2023، صفحة 12)

ث. الاحتيال النظيف

وهو من أخبث أنواع الاحتيال، فهو يتم بطريقة قانونية نظيفة وبدون ترك أي مجال للمحاسبة القانونية، حيث يوقع المجرم الضحية في الفخ من خلال وضعه في دائرة القانون وسرقة أمواله منه بدون ترك حق المطالبة بأمواله له، فبعض الأشخاص يشتركون بمواقع الإعلانات التي تعطي عمولة على مشاهدة الإعلانات و **الاحتيال** توهمهم بأنها تقدم لهم أرباح يومية عند استقدام عملاء جدد بنظام "الريفل" وباستخدام طريقة بونزي للاحتيال. (عبدو، 2021)

2. أساليب الإحتيال الإلكتروني

لتنفيذ العمليات الاحتيالية من طرف المحتالين فإنهم يلجئون إلى مجمعة الطرق والأساليب التي يستخدمونها ومن بين هاته الأساليب لدينا:

أ. الاحتيال التجاري

ويكون هذا الاحتيال خلال عمليات البيع والشراء المختلفة عبر المتاجر الالكترونية غير الموثوقة.

ب. الإحتيال بوسائل الاتصال

استغلال وسائل الاتصال لسرقة الأموال من العملاء أو مزوّدي خدمة الاتصالات أو كلاهما.

مثال: استخدام رقم الجوال في التواصل مع الأفراد وخداعهم بأنهم ممثلو خدمة العملاء لدى البنوك أو بعض شركات مزودي الخدمات بهدف التهديد والابتزاز و سرقة الأموال والمعلومات الشخصية. (هيئة الحكومة الرقمية,، 2023)

ت. إحتيال رسائل البريد الالكتروني

هو طريقة من طرق الاحتيال الالكتروني يتم فيها إرسال رسائل مضللة ومزيفة للمستخدم بغرض خداعه والحصول منه مبالغ مالية أو علي معلومات وبيانات الهوية الشخصية مثل رقم بطاقة الائتمان أو الحساب المصرفي وهناك أنواع عديدة العروض التي تتضمنها رسائل البريد الالكتروني الاحتيالية . (شهيرة و سويح، 2019، صفحة 39)

- **إستدعاء عاجل لاتخاذ إجراء أو تهديدات :**

إشتبه في رسائل البريد الإلكتروني ورسائل Teamsالتي تدعي أنه يجب النقر فوق مرفق أو الاتصال به أو فتحه *على الفور*. في كثير من الأحيان، سيطالبون بأن عليك التصرف الآن للمطالبة بمكافأة أو تجنب عقوبة. *إن خلق شعور زائف* بالإلحاح هو خدعة شائعة لهجمات التصيد الاحتيالي والرسائل الخادعة. يفعلون ذلك حتى لا تفكر في الأمر كثيرا أو تتشاور مع مستشار موثوق به قد يحذرك. (موقع قوقل ماسكروسوفت)

- **الاعتداء علي المعطيات:**

الاعتداء علي المعطيات يعتمد في ذالك علي تقنية الاختراق كذالك أو ما يعرف بhaking بغرض الدخول علي المعطيات السرية و المحمية أو الخصوصية الشخصية وعلي البيانات التي لها صفقة بالحياة الفردية من خلال استخدام الانترنت والغرض من ذالك التزوير أو الاختلاس أو تحقيق غايات شائنة ما يجعل هذه الاعتداءات حديث المجالس والاجتماعات و الرسائل الإعلامية والأجهزة الأمنية. (شهيرة و سويح، 2019، صفحة 40)

ث. **احتيال التسويق**

عندما يتسوق المستخدمون علي الانترنت فإنهم يكونون فريسة سهلة للمحتالين الذين ينتشرون عبر الشبكة العنكبوتية ويستعمل المحتالون في الانترنت أساليب وطرق كثيرة لخداع المتسوقين كأن يضعوا لهم إعلانات وهمية عن بضائع لايمتلكونها وليست موجودة عندهم وعند رغبة المستهلك بشرائها يتم طلب إدخال تفاصيل البيانات الشخصية وعند إدخالها يقومون بعملية النصب. (ناصر)

ج. **التجسس علي الحياة الخاصة**

نعني به الاطلاع علي حياة الأشخاص وخصوصياتهم من دون علمهم بذالك ودون إذنهم وهي من الآفات السيئة من الناحية الاجتماعية والأخلاقية ولا يختلف التجسس عن الاختراق إلا من حيث الهدف لان الأساليب المتبعة هي نفسها يراد من خلاله تمكين المتجسس من التعرف علي محتويات الحاسوب المستهدف. (شهيرة و سويح، 2019، صفحة 13)

تعددت أسباب الاحتيال الالكتروني ويأتي في مقدمتها نمو منصات التواصل الاجتماعي وارتفاع عدد مستخدمي الانترنت في العالم إلى 5,16 مليارات شخص في 2023 إي ما يقارب 64,6 % من سكان الكرة الأرضية مما شكل بيئة خصبة للمحتالين ومروحة واسعة من الشرائح الاجتماعية المستهدفة. (الصنديد)

ثالثا: أسباب الاحتيال الالكتروني وطرق الحماية منه

1. أسباب الإحتيال الإلكتروني

كل مرة نتعرض فيها أو نسمع بها عن عملية احتيال إلكتروني نسأل أنفسنا عن دافع الجهات الخبيثة لارتكاب هذا الجرم، والذي يُصنَّف ضمن الاستخدام الخاطئ لشبكة الإنترنت ومنصات التواصل الاجتماعي؛ لذا فإنَّنا نوضِّح لكم أسباب الاحتيال الإلكتروني:

- نمو منصات التواصل الاجتماعي وارتفاع عدد مستخدمي الإنترنت في العالم إلى 5.16 مليارات شخص في 2023، أي ما يقارب 64.6% من سكان الكرة الأرضية، مما شكّل بيئة خصبة للمحتالين ومروحة واسعة من الشرائح الاجتماعية المستهدفة. (الصنديد)
- قلة الوعي عند الأفراد عن مفهوم الاستخدام الصحيح والمفيد لشبكة الإنترنت ووسائل التواصل الاجتماعي.
- المكاسب المالية: يمثل تحقيق المكاسب المالية من خلال سرقة البيانات الشخصية ، أو ابتزاز الضحايا، أو اختراق الحسابات المصرفية ، او نشر برامج الفدية ، الدافع الرئيسي وراء الاحتيال الالكتروني. (موقع الكتروني،اسباب و انواع الجرائم الالكترونية و سبل مكافحتها ، 2025)
- ضعف أنظمة الأمن والخصوصية الإلكترونيين لدى بعض الشركات، ممَّا يسهِّل اختراق بياناتهم من قبل بعض العابثين وابتزاز أصحاب هذه البيانات وشركاتهم. (وان)

من جهة أخرى تسهم قلة الوعي بالمخاطر المعلوماتية وضعف تدابير الأمن السيبراني لدى العديد من المستخدمين في زيادة فرص انتشار ونجاح المحاولات الاحتيالية، هذا بالإضافة إلى التطور المستمر في تقنيات الاحتيال، إذ يحرص المحتالون على تطوير أساليبهم لاستهداف الأفراد والمؤسسات بشكل أكثر تعقيدًا. (الصنديد)

- الشراء من متاجر إلكترونية غير موثوقة، ومن ثمَّ حدوث عمليات نصب وسرقة الأموال أو غش في مواصفات المواد.
- انتشار العملات الإلكترونية الاحتيالية، والتي تندرج ضمن أنواع الاحتيال النظيف الذي تحدَّثنا عنه، فهي لا تترك للضحية أي مجال للشكوى أو التظلُّم أو استرداد أمواله. (وان)

وقد كشف استطلاع للرأي أجرته شركة الاستشارات البريطانية «مان بايتس دوغ» في سبتمبر الماضي أن الشركات تواجه تهديدًا مزدوجًا من الجرائم الإلكترونية، فمن جهة، يتمكن القراصنة من اختراق أنظمة الشركات عبر نقاط ضعف في الخوادم السحابية، ومن جهة أخرى، يمثل الموظفون أنفسهم خطرًا كبيرًا، حيث يمكن خداعهم للكشف عن معلومات حساسة أو تنفيذ إجراءات ضارة. (الصنديد)

- سرقة بيانات حساسة عن الأفراد موجودة في بيانات شركاتهم ومؤسساتهم، واستغلال هذه البيانات في معظم الجوانب، كأن تُسرق قاعدة بيانات جامعة إلكترونية من أجل الحصول على أسئلة الاختبارات، ثمَّ إيجاد بيانات متعلقة بالحسابات المصرفية للمدرسين تُحوَّل أجورهم إليها، فتُستغل هذه البيانات في عمليات الاحتيال. (وان)

بهدف الحماية من براثن الاحتيال الإلكتروني المتزايد، يقتضي اتخاذ مجموعة من التدابير الوقائية: كتجنب مشاركة المعلومات الشخصية الحساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر قنوات غير آمنة أو مع جهات غير موثوقة، إضافة إلى التحقق من صحة الروابط والملفات المرفقة قبل فتحها، خاصة في الرسائل الإلكترونية التي تبدو مشبوهة أو تأتي من مصادر غير معروفة، ناهيك عن وجوب استخدام كلمات مرور قوية ومميزة لكل حساب مع تغييرها بانتظام.

وبالطبع، هناك حاجة ماسة لبناء وتعزيز الوعي الرقمي من خلال متابعة آخر التطورات في مجال الأمن السيبراني والتعرف على أحدث أساليب الاحتيال الإلكتروني (الصنديد)

- الجهل بمواقع الإنترنت والدخول إلى مواقع غير آمنة ضمنها (وان)

تبذل الجهات المعنية في القطاعين العام والخاص في الكويت جهودًا حثيثة لتعزيز الأمن الرقمي، فإلى جانب هيئة الاتصالات وتقنية المعلومات، والمركز الوطني للأمن السيبراني، وإضافة الى ما تقوم به وزارة الداخلية ووزارة الإعلام من جهود تخدم الاستراتيجية الوطنية للأمن السيبراني، لا تتوانى الشركات الخاصة ولا سيما البنوك والمؤسسات المالية عن إطلاق حملات إعلامية توعوية للمتعاملين. (وان)

2. طرق الحماية من الاحتيال الإلكتروني

يجب على الأفراد أن يكونوا يقظين عند استعمالهم لمواقع الانترنت ووسائل التواصل الاجتماعي من أجل ضمان حماية أنفسهم لعدم الوقوع ضحية في جرائم الاحتيال الإلكتروني، ومن ابرز هذه الطرق:

- اتخاذ إجراءات السلامة والأمن على شبكة الانترنت لزيادة تحديث أنظمة التشغيل أولا بأول لحماية نظام الحاسوب.
- التعامل بحذر شديد مع الرسائل التي تأتي من مصادر مجهولة وعدم الضغط على أي روابط مجهولة. (وان)

3. أساليب الأمن المعلوماتي :

يمكن تجنب العديد من الاعتداءات التي تتعرض لها البيانات والمعلومات المدونة إلكترونيا، والتحكم في الدخول اليها إلا لمن له الحق بذلك ، وفقا لمجموعة من الآليات الدفاعية التي تمنع حدوث الاحتيال والاختراق للمواقع والبيانات من خلال (شهيرة و سويح، 2019، صفحة 43):

- التحكم بالدخول للأصول المعلوماتية:

يكون هذا الإجراء عن طريق جهاز رقابة إيجابي يقوم بتحديد عما إذا كان الشخص طالب الدخول مصرحا له بذالك أم لا والعمل بموجب، كما يقوم هذا الجهاز الإيجابي بالتحري عن شخصية المتصل بربط عملية تصريح الدخول والتحري عن الشخصية فتكون سرية المعلومات مضمونة وغير متاحة للكافة للإطلاع عليها، أو لاحتيالها بغير وجه حق . (شهيرة و سويح، 2019)

- الإبلاغ عن الجرائم فور حصولها والتواصل مع الجهات المسؤولة:

وفي حال تعرضكم لأي مشكلة أو احتيال الكتروني يمكنكم التواصل مع شركة سايبر وان المتخصصة في مجال الأمن السيبراني من أجل تقديم المساعدة اللازمة لكم بسرية تامة وبسرعة كبيرة.

- عدم التجاوب مع رسائل الفوز بالجوائز أو شركات التسويق. (وان)
- اكتشاف التطفل وسوء الاستخدام :

يهدف اكتشاف التطفل إلى اكتشاف النشاط الضار في بدايته ويتحقق ذلك عن طريق مراقبة النشطة الحالية أو مراجعة القوائم التي يتم تسجيل هذه النشطة فيه، وإن تم الاكتشاف في وقت مبكر يمكن إجهاض محاولة الاعتداء قبل حدوث الضرر، وحتى في حالة عدم التمكن من إيقاف النشاط فالعلم به بحد ذاته ينبئ مسؤولي الأمن إلي الثغرات المنية لتلافها. (شهيرة و سويح، 2019، صفحة 43)

يتمثل ترشيح المعلومات في وجود برنامج أو جهاز يقوم بمراقبة المعلومات الداخلية والخارجية من شبكة الحاسب الآلي، ينبني هذا القرار على المعلومات في مقدمة الرسالة المرسلة التي تشمل عناصر أساسية خاصة بالمرسل كالعنوان، ونوع الخدمة بالانترنت بريد الكتروني، ويب وغيرها، وتتجسد هذه المرشحات في كل من جدار الحماية الأمنية . (شهيرة و سويح، 2019، صفحة 43)

- إدخال المعلومات الشخصية عبر المواقع الموثوقة والانتباه عند كتابة المعلومات الشخصية على شبكة الانترنت.
- تحديث برامج الحماية على الحواسيب.
- تجاهل الروابط المجهولة.
- رفض الرسائل الخاصة بطلب قبول تثبيت برامج مجهولة.
- استعمال برامج الحماية من الفيروسات.
- التأكد من صحة الرسائل التي تكون باسم البنوك ومراجعتها قبل إتمام أي عملية. (وان)

4. وسائل تحقيق الأمن المعلوماتي

إعداد معايير امن عالمية تكون منسجمة ومتوافقة مع التطبيق الجغرافي المتسع والممتد على أوسع نطاق علي العالم حيث يمثل تطوير توجيهات ومعايير الأمن المنتج التعاوني بين الحكومات والمنظمات والمنتجين والموردين والمستخدمين لنظم المعلومات. (شهيرة و سويح، 2019، صفحة 44)

- تحديث برامج الحماية على الحواسيب.
- تجاهل الروابط المجهولة.
- رفض الرسائل الخاصة بطلب قبول تثبيت برامج مجهولة. (وان)

تفتيش المنظومات المعلوماتية: سمح المشروع للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ، منظومة تخزين معلوماتية أخرى وان هذه المعطيات يمكن الدخول إليها

رابعا: أشهر طرق الاحتيال عبر تطبيق بريدي موب

1. تعريف تطبيق بريدي موب

هو تطبيق الكتروني تابع لمؤسسة بريد الجزائر انشأ سنة 2018 ومتوفر علي متجري التطبيقات بلاي ستور و ابل ستور وهو عملية تطبيقية علي الهاتف النقال تضع تحت تصرفكم الخدمات النقدية والمالية لبريد الجزائر وبالتالي فهي تساهم في تحسين الاستخدام الأكفأ للوقت والتسيير الأحسن لحسابكم البريدي الجاري ولمعاملاتكم المالية كيفما وحيثما شئتم. (العمري، 2023)

2. شروط الاستفادة من تطبيق بريدي موب

للاستفادة من خدمات بريدي موب يجب الدخول إلى الموقع الرئيسي الخاص ببريد الجزائر و بعدها الضغط علي خانة تنزيل أو تحميل تطبيق بريدي موب عند الضغط عليها سوف يأخذك مباشرة إلي "بلاي ستور "، بعدها قم بتحميل التطبيق وتثبيته على جهازك .

أدخل المعلومات المطلوبة الخاصة بك: رقم هاتفك شرط أن يكون نفسه الذي قمت بفتح به البطاقة الذهبية، تاريخ انتهاء الصلاحية، 16 رقم الموجود على البطاقة و الرقم الموجود خلفها مكون من ثلاث أرقام، بعدها قم بتأكيد وإرسال المعلومات أي تسجيل، ستقوم آلجي بوسط بإرسال كود التأكيد قم بإدخاله فبذالك تكون قد أتممت عملية التسجيل. (وثائق المؤسسة)

3. خدمات تطبيق بريدي موب

- خدمة تحويل المبالغ المالية من حساب إلى حساب .
- خدمة الاطلاع عن الرصيد وكشف العمليات الأخيرة المصغرة .
- خدمة تعبئة رصيد الهاتف النقال لمختلف المتعاملين (جيزي، موبيليس، أوريدو) .
- تجميد المؤقت للبطاقة وإعادة التشغيل .
- تعقب الرسائل والطرود .
- تسيير البطاقة الذهبية والاستفادة من خدماتها .
- خدمة سحب المال من الصراف الآلي دون إظهار أو استخدام البطاقة الذهبية.
- خدمة تعبئة الانترنت adsl.
- تحديد مواقع المكاتب البريدية وكذا الموزعات الآلية لنقود . (العمري، 2023)
- خدمات بريدي باي أو ما يعرف برمز الاستجابة السريعة .

بريد الجزائر www.poste.dz

تسعي مؤسسة بريد الجزائر جاهدة في حماية المواطنين من كافة أشكال النصب والاحتيال التي يمكن أن يتعرضوا إليها من خلال إصدار العديد من الإجراءات الرامية إلى تامين الممتلكات المادية الخاصة بزبائنها حيث جندت الوزارة بالتنسيق مع العديد من القطاعات جميع مصالحها لأجل تحسيس زبائنها بضرورة اخذ الحيطة والحذر فيما تعلق بالمعاملات المالية.

وهناك العديد من التقنيات الخادعة المساهمة في تسهيل عمليات الاحتيال حيث أصدرت مؤخرا المنظمة الجزائرية لحماية وإرشاد المستهلك تحذيرا عاجلا لمستخدمي تطبيق بريدي موب التابع لبريد الجزائر من تصاعد محاولات الاحتيال الالكتروني التي تهدد بسرقة بياناتهم المالية ونبهت المنظمة إلى أن

هاته الهجمات باتت أكثر تطورا حيث يستخدم المحتالون تقنيات خادعة وانتحال صفة موظفي بريد الجزائر لتنفيذ جرائمهم .

وسائل التواصل الاجتماعي احد وسائل النصب بدورها أضحت وسائل التواصل الاجتماعي ابرز سبل النصب والاحتيال الالكتروني بالنظر إلى وصولها لأكبر شريحة من المواطنين وكذا دخولها العديد من المجالات ومن أبرزها التجارة التي تروج عبر هاته الوسائل من طرف أشخاص مجهولين متخفيين وراء الشاشة حيث يعمل بعضهم علي إيهام رواد مواقع التواصل الاجتماعي بتوفر بضاعة معينة وهو الأمر الذي كثيرا ما تنبه عنه الوزارة.

4. طرق الإحتيال عبر تطبيق بريدي موب

من أبرز طرق عمليات الاحتيال الإلكتروني التي تتم عن طريق بريدي موب تمثلت في:

- **طلب الرقم السري:** يدعي المحتالون وجود مشكلة في الحساب ويطلبون من الضحية تقديم الرقم السري الخاص بالحساب بحجة إصلاح المشكلة .
- **طلب الرمز المرسل:** عبر حديث يطلب المحتالون من الضحية تزويدهم بالرمز الذي يتلقاه عبر رسالة نصية قصيرة من بريد الجزائر. (هواري، 2025)

انتشرت مؤخرا طريقة من ضعاف النفوس للنصب على الغير و عن طريق البريدي موب لذلك أردت أن أحذركم حتى لا تتعرضوا للنصب و الاحتيال.

الطريقة هي أن هناك بعض الأشخاص يشترون رسائل sms من شركات الاستضافة كOVH مثلا يستعملونها في إرسال رسائل لأي هاتف في العالم كما أنها تتيح لهم اختيار العنوان. (طريقة جديدة للنصب والإحتيال عبر تطبيق بريدي موب، 2020)

لذلك يقومون بحجز المبلغ من عند البائع و يرسلون له رسالة تأكيد وصول المبلغ لرقم هاتفه تماما مثل الرسالة التي يرسلها البريد ALG POSTE و هنا بكل تأكيد سيقوم البائع بتحويل اليورو إلى حساب النصاب **طلب صورة البطاقة الذهبية** يزعم المحتالون أنهم بحاجة إلى صورة للبطاقة الذهبية لتفعيلها وهو طلب وهمي لا يمت للحقيقة بصلة. (هواري، 2025)

5. نصائح مهمة للمستخدمين

تسعى دائما مؤسسة بريد الجزائر إلى حماية مستخدميها لتطبيق بريدي موب لتوفير حماية أكثر لعدم التعرض للهجمات الاحتيالية الإلكترونية وتقديم مجموعة من الإرشادات والنصائح لعدم الوقوع ضحية لتلك الهجمات ومن أبرز هاته النصائح:

- عدم مشاركة المعطيات الشخصية مع أي كان، لاسيما: الاسم واللقب، رقم البطاقة الذهبية، الرقم السري، كلمة المرور ذات الاستخدام الوحيد.
- التأكد من تحميل وتنصيب التطبيقات الرسمية.
- تجميد البطاقة وتقديم شكوى لدى مصالح الأمن المختصة في حالة التعرض للنصب أو الإحتيال. (حملة تحسيسية من أجل إستخدام آمن للبطاقة الذهبية وتطبيق بريدي موب)
- عدم مشاركة المعلومات الشخصية والحذر ممن يدعون تمثيل بريد الجزائر ويطلبون معلومات حساسة.
- لا ينبغي مشاركة الرقم السري أو أي بيانات مالية عبر الهاتف أو الرسائل.
- الاتصال بالرقم الرسمي لمصلحة بريد الجزائر للتأكد من صحة الطلبات التي تصلهم.
- تجنب النقر على الروابط التي قد ترد عبر الرسائل النصية أو تطبيق واتساب. (هواري، 2025)

المبحث الثاني: مواقع التواصل الاجتماعي

أولا: تعريف مواقع التواصل الاجتماعي

1. نشأة ومفهوم مواقع التواصل الاجتماعي

إن نشأة مواقع التواصل الاجتماعي ظهرت مع الشبكة العنكبوتية العالمية (الإنترنت) والتي أحدثت نقلة تاريخية في مجال التواصل البشري وأسهم في نقل الإعلام إلى آفاق غير مسبوقة وأعطت مواقع التواصل وشبكاته المستخدمين فرص كبرى لتأثير والانتقال عبر الحدود بلا رقابة إلا بشكل نسبي محدود. (قاسمي و جداي، 2019، صفحة 18)

ففي عام 1995 ظهر أول موقع اجتماعي تواصلي وهو موقع (Classmates.com) الذي صمم من قبل راندي كونرادر، حيث كان الهدف منه مساعدة الأصدقاء والزملاء الذين جمعتهم الدراسة في مراحل حياتية معينة وفرقتهم ظروف الحياة العملية في ما كان متباعدة ،كما أنه يلبي رغبة هؤلاء الأصدقاء والزملاء في التواصل فيما بينهم إليكترونيا. (العالي و آخرون، 2016، صفحة 206)

ثم ظهر موقع six Degrees.comوالذي أخذ أسمه من عبارة Sparation Six Degrees of أي بمعنى ستة درجات من الانفصال، والتي أخذت من تجربة العالم الصغير لعالم النفس الأمريكي في جامعة هارفاد " لستاتي مليغرام". (فيصل محمد)

وقد ركز هذا الموقع على الروابط المباشرة لأشخاص ولم يولي اهتماما للانتماءات العلمية والعرقية ، كما أنه أتاح للمستخدمين مجموعة من الخدمات أهمها آنساء الملفات الشخصية ، وإرسال واستقبال الرسائل الخاصة لكن تم إغلاقه مع نهاية عام 2000 لأنه لم تأتي بأرباح لمالكيها . (فضل الله، 2010، صفحة 7)

وتبع ذالك مجموعة من مواقع التواصل الإجتماعي خلال الفترة 1997-1999 وكان محور إهتمامها هو تدعيم المجتمع من خلال مواقع تواصل اجتماعية مرتبطة بمجموعات معبنة مثل موقع الأمريكيين الأسيويين Asian Venue com، وموقع البشر ذو البشرة السمراء Black planet .com ليتولي ظهور موافع أخرى منها: مواقع لايف جورنال ، وموقع كاي ورلد عام 1999. (قاسمي و جداي، 2019، صفحة 18)

وحسب الدراسات والأبحاث المقدمة لمواقع التواصل الاجتماعي يعتبر عام 2002 الميلاد الفعلي لمواقع التواصل الاجتماعي، كما نعرفها اليوم فمع بدايته أنشأ موقع Friendsten.com من قبل Jonathan – Abrams وهو وسيلة للتعارف وتشكيل الصداقات بين مختلف فئات المجتمع العالمي، وفي النصف الثاني من العام ظهر موقع Skyrock.com في فرنسا كمنصة للتدوين وقد تحول بشكل كامل إلى موقع اجتماعي تواصلى عام 2007، وتلاهما موقع My Scpace .com الأمريكي المشهور عام 2003.

والذي كانت له شعبية كبيرة في العالم، حيث أصبح أكبر موقع تواصلي إجتماعي عام 2006 يقدم تفاصيل الملفات الشخصية التي تتضمن عرض الشرائح ومشغلات الصوت والصورة بالإضافة إلى خدمات التدوين. (الشمالية و آخرون، 2015، صفحة 201)

وكما ظهرت بالتوازن العديد من مواقع التواصل الاجتماعي منها موقع Linkedin.comالذي أطلق رسميا في الخامس من ماي عام 2003 ووصل عدد مستخدميه إلي 250 مليون مشتركا بنهاية شهر ديسمبر 2012 .(المصري، 2011، صفحة 43)

2. مفهوم مواقع التواصل الإجتماعي

تعددت واختلفت المفاهيم حول مفهوم مواقع التواصل الاجتماعي فكل باحث لديه تعريف خاص لها نتطرق في الآتي إلى مجموعة من المفاهيم والتعريفات:

لغة : قسمت ستيال هيلجاتو Helgadottir.s مصطلح وسائل التواصل الاجتماعي إلى جزئين media social، الجزء الأول كلمة mediaوتعني وسيلة من وسائل الإعلام التي تتيح تواصل الأفراد معا بما في ذلك الوسائل التقليدية كالراديو والتلفزيون والصحف ،بينما كلمة social تعني أن العملية الاتصالية تسير في اتجاهين من المرسل إلى مستقبل الرسالة وفي اللحظة نفسها من المستقبل إلى المرسل كرد الفعل . (الهاشمي و آخرون، 2020، صفحة 50)

اصطلاحا:

مواقع التواصل الاجتماعي عبارة عن تطبيقات تكنولوجية مستندة إلى الويب تتيح التفاعل بين الناس وتسمح بنقل البيانات الإلكترونية وتبادلها بسهولة، وتوفر للمستخدمين إمكانية العثور على آخرين مشتركون ،في نفس المصالح وبناء عليه ينتج عن ذلك ما يسمى بالمجتمعات الافتراضية، حيث يستطيع المستخدمون التجمع في كيانات اجتماعية تشبه الكيانات الواقعية. (علي سيد، 2019-2020، صفحة 20)

مواقع التواصل الاجتماعي التعريف: هي عبارة عن عدة شبكات إلكترونية يتم من خلالها التواصل فيما بين الأفراد سواء داخل الدولة أم على المستوى العالمي تجمع بين العديد من الشباب الذين تتلاقى اهتماماتهم نحو موضوع معين أو هواية معينة يمارسونها من خلال مواقع التواصل الاجتماعي. (راضي، 2003، صفحة 23)

عرفت بأنها عبارة عن تجمعات اجتماعية من خلال شبكة الانترنت يستطيع روادها القيام بمناقشات خلال فترة زمنية مفتوحة يجمعهم شعور أنساني طيب وذالك في إطار محدد. (حداد، 2002، صفحة 23)

حسب بويد واليسون مواقع شبكات الاجتماعية هي خدمات عبر شبكة الانترنت تسمح للإفراد بناء شخصية عامة او شبه عامة من خلال نظام محدد توضيح لائحة خاصة بالمستخدمين الذين يشاركوكم الاتصال عرض واختيار قائمة الاتصالات الخاصة والقوائم الخاصة بالاخرين خلال نفس النظام (نيكول و بويد، 2007، صفحة 230) .

وكما عرفها محمدي مواقع التواصل الاجتماعي بأنها منظومة من الشبكات الالكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به وبعد ذالك يجري ربطه عن طريق نظام اجتماعي الكتروني مع آخرين لديهم اهتمامات وهوايات متشابهة أو نفسها وهذا الترابط نتج عنه نوع من التواصل يختلف عن أنظمة التواصل التقليدية القديمة وهو ما عرف بوسائل الإعلام الاجتماعي أو وسائل الإعلام البديلة. (محمدي، صفحة 47)

ويعرفها إيهاب خليفة على أنها مواقع تتشكل من خلال الانترنت تسمح للأفراد بتقديم لمحة عن حياتهم العامة وإتاحة الفرصة للاتصال بقائمة المسجلين والتعبير عن وجهة نظر الإفراد أو المجموعات من خلال عملية الاتصال وتختلف طبيعة التواصل من موقع لآخر. (خليفة، 2016)

وكما يعرفها حسين شفيق على أنها: مواقع على الانترنت يتواصل من خلالها ملايين من البشر الذين تجمعهم اهتمامات أو تخصصات معينة ويتاح لأعضاء هذه الشبكات مشاركة الملفات والصور وتبادل مقاطع الفيديو وإنشاء مدونات وإرسال رسائل وإجراء محادثات فورية .(شفيق)

وتعرفها هبة خليفة بأنها مجموعة من صفحات الويب تسهل التفاعل الناشط بين الأعضاء المشتركين في الشبكة الاجتماعية الموجودة بالفعل على شبكة الانترنت تهدف إلى توفير مختلف وسائل الاهتمام التي تساعد الأعضاء المشتركين على التفاعل بين بعضهم البعض. (يعقوب، 2015، صفحة 30)

3. خصائص مواقع التواصل الاجتماعي

- إمكانية التحدث مع أكثر من مستخدم في نفس الوقت.
- الهامش الكبير من الحرية في التعبير عن الاهتمامات والآراء.
- تتيح التواصل خارج حدود المنطقة والدولة او بما يعرف بكسر الحواجز المكانية في التواصل.
- التركيز على بناء العلاقات ابتداء بالتعارف ووصولا إلى ربط علاقات متينة، وهذا بفضل ما توفره مواقع شبكات التواصل الاجتماعي من خدمات تخلق عالم افتراضي تقني يحاكي الواقع بعطيات العصر الحديث من التقنية المتقدمة. (نبيلة و بن تومي، 2014، صفحة 540)

ثانيا: دورها في انتشار الاحتيال

4. دور مواقع التواصل الاجتماعي في انتشار عمليات الاحتيال الالكتروني

بانتشار وتعدد مواقع التواصل الاجتماعي اختلفت وظهرت طرق وأساليب جديدة ووسائل للاحتيال الالكتروني وذالك يعود إلى مجموعة من الأسباب منها سهولة إنشاء الحسابات الوهمية وانتشار الإعلانات المظللة وضعف الوعي الأمني لدى بعض المستخدمين أولا.

الفرص المتزايدة: إن ازدياد عدد مستخدمي الحاسوب من ذوي المعرفة والمقدرة في اختراق البيانات نتيجة لا مركزية المعالجة الشبكات الاتصالية والدخول عن بعد إلى الحاسوب قد اتخذت فرصا متزايدة للمزورين والمتلاعبين لتنفيذ أغراضهم لاسيما في ظل سيطرة ورقابة غير كفئة في هذا المحيط الالكتروني لمعالجة البيانات.

تحقيق أرباح كبيرة: نتيجة للأرباح الطائلة يمكن ان يجنيها مرتكب عملية الاحتيال وذالك بالتزوير والتلاعب فإنها تشكل دفاعا قويا لأصحاب النوايا السيئة في ارتكاب جريمتهم في استبيان اجراه احد الباحثين في امريكا عام 1995بين معدل ارباح مرتكب عملية الاحتيال عبر الحاسوب وصلت 600,000 دولار مقابل 300,000 دولار لمرتكب الجريمة في النظام اليدوي. (Fnancial fraud exploring types and beyond)

صعوبة الاكتشاف: إن وجود كم كبير من البيانات المخزنة في الحاسوب يجعل إخفاء أي تزوير أو تلاعب عملية سهلة خاصة إذا تمكن مرتكب الجريمة من عدم ترك اي دليل خلفه الأمر الذي يترتب عليه صعوبة اكتشاف الجريمة.

ثالثا: أشهر المنصات التي يتم عليها الإحتيال

أصبحت مواقع التواصل الاجتماعي أرضا خصبة بالنسبة للمحتالين لتنفيذ عملياتهم الاحتيالية وذالك باستغلال القاعدة الضخمة للمستخدمين بالإضافة إلى الخدمات المشروعة والأدوات التسويقية وعلي الرغم من الجهود المبذولة للحد من الأنشطة الاحتيالية فإنها مستمرة في الصعود.

ولقد كشفت لجنة التجارة الفدرالية أن أكثر الخسائر التي تم الإبلاغ عنها بسبب الاحتيال عبر وسائل التواصل في النصف الأول من عام 2023 كانت من أشخاص حاولوا شراء شيء من خلال إعلان علي فيسبوك أو انستغرام . (اسماعيل، 2024)

- فيسبوك Facebook

هو شبكة اجتماعية استأثرت بقبول وتجاوب كبير من الناس خصوصا من الشباب في جميع أنحاء العالم، وهي لا تتعدى حدود مدونة شخصية في بداية نشأتها في شباط عام 2004 .

في جامعة (هارفارد) في الولايات المتحدة الأمريكية، من قبل طالب يدعى مارك زوكربيرج، فتحت شهرتها حدود الجامعة (خليفة، 2016، صفحة 114)، وانتشرت في مدارس الولايات المتحدة الأمريكية المختلفة ، وظلت مقتصرة على أعداد من الزوار، حتى عام 2007.

حيث حقق القائمون على الموقع إمكانات جديدة لهذه الشبكة ومنها، إتاحة فرصة للمطورين مما زادت هذه الخاصية من شهرة موقع فيسبوك بحيث تجاوز حدود الولايات المتحدة الأمريكية إلي كافة أنحاء العالم، وتجاوز عدد المسجلين في هذه الشبكة في الأول من تموز 2010 النصف مليار شخص يزورونها باستمرار ويتبادلون فيما بينهم الملفات والصور ومقاطع الفيديو ويعلقون على ما ينشر في صفحاتهم من آراء وأفكار وموضوعات متنوعة وجديدة، يضاف إلى ذالك المشاركة الفعالة، وغالبا ما تكون في المحادثة والدردشات.

و تحتل شبكة الفيس بوك حاليا من حيث الشهرة و الإقبال المركز الثالث بعد موقعي قوقل (مايكروسوفت) وبلغ عدد المشتركين فيها أكثر من (800) مليون شخص. (بن ابراهيم، 2015، الصفحات 63-64)

علي الرغم من أن فيسبوك بات وسيلة شائعة للإعلان عن المنتجات وبيعها إلا أن منصة التواصل الاجتماعي تشهد تزايدا في نشاط المحتالين إذ بات البعض يستخدم أساليب مختلفة لخداع الضحايا. (كوميبتون، 2024)

وذالك من خلال الإعلانات الاحتيالية التي تملا المنصة مع وجود مليارات المستخدمين الذين يشاركون تفاصيلهم الشخصية عبر الانترنت أصبح بإمكان المحتالين استهداف شرائح معينة بسهولة باستخدام أدوات إعلانات مطورة وكما يمكن من جهة أخرا لأي شخص إنشاء حساب وبدء الإعلان مع الحد الأدنى من التحقق مما يسهل على المحتالين إنشاء وتوزيع إعلانات مزيفة. (اسماعيل، 2024)

وكما يستغل المحتالون أدوات التسويق الشرعية التي توفرها منصات التواصل مستفيدين من خوارزمياتها لتوسيع نطاق إعلاناتهم لتصل إلى اكبر عدد من المستخدمين.

العملات الرقمية المشفرة لعبت هاته الاخيرة دورا كبيرا في عمليات الاحتيال الاستثمارية التي ابلغ عنها حيث اظهرت اكثر من نصف التقارير ان الضحايا دفعوا للمحتالين عن طريق العملات المشفرة عبر مواقع التواصل . (اسماعيل، 2024)

- انستغرامinsregram

الإعجاب، وهو من المواقع التي اكتسبت شعبية علي المستوى الفردي والمؤسسي، والانستغرام تطبيق متاح لتبادل الصور إضافة إلى أنها شبكة اجتماعية .

كانت بداية انستغرام عام 2010م حينما توصل إلى تطبيق يعمل على التقاط الصور و إضافة فلتر رقمي إليها وإرسالها عبر خدمات الشبكات الإجتماعية .

وكما تتم عملية الإحتيال عبر منصة فيسبوك كذالك تتم عملية الاحتيال عبر منصة انستغرام وهذا بسبب صعوبة اكتشاف هاته الإعلانات الاحتيالية رغم وجود سياسات لمنع الإعلانات الاحتيالية فان منصات التواصل الاجتماعي غالبا ما تواجه صعوبة لتطبيقها بشكل فعال إذ أن الإعلانات الاحتيالية تتجاوز المراجعات من خلال مجموعة من التكتيكات سنقوم بذكرها :

- استغلال الثغرات.
- وجود طرف ثالث في صناعة الإعلانات.
- كثرة الإعلانات.
- استخدام التزييف العميق.
- الشرعية المزيفة.
- الاستهداف المحلي. (اسماعيل، 2024)

رابعا: طرق الحماية من الاحتيال عبر المواقع

1. طرق الحماية من عمليات الاحتيال الالكتروني

لتعرف علي عمليات الاحتيالية عبر مواقع التواصل الاجتماعي أمر بالغ الأهمية من اجل حماية نفسك وأموالك حيث تفشل جهود مراقبة الإعلانات لا يمكنها اكتشافه.

ومن ابرز الخطوات التي يجب إتباعها لحماية نفسك من الوقوع في عملية نصب واحتيال

- **تحقق من الحسابات الموثوقة** : تأكد من أن الحسابات التي تتفاعل معها تمثل الجهات الرسمية من خلال العلامة الزرقاء أو مراجعة المعلومات الموثوقة مثل الموقع الالكتروني. (البنك السعودي للإستثمار، 2025)
- **تحقق من هوية المرسل في الرسائل الإلكترونية:** قد تبدو رسائل البريد الإلكتروني موثوقة للوهلة الأولى ، لكنها غالبا ما تحتوي على تفاصيل تكشف زيفها عند الفحص الدقيق .

وعند التدقيق ، قد تجد أن عنوان البريد الإلكتروني يختلف قليلا عن العنوان الرسمي للشخص أو الشركة. (تلفزيون سوريا)

- **استخدام المصادقة الثنائية** : إضافة طبقة أمان إضافية إلى حساباتك يمكن أن يجعل من الصعب علي المحتالين الوصول إلي معلوماتك. (البنك السعودي للإستثمار، 2025)
- **تحديث الأجهزة الرقمية باستمرار**: ينبغي على المستخدمين تحديث أجهزتهم الرقمية بشكلٍ مستمر، سواءً كانت أجهزة حاسوبية أو أجهزة خلوية، وذلك لإصلاح الثغرات والعيوب الأمنية الّتي يستغلها المجرم الإلكتروني للوصول إلى المعلومات الشخصية والمالية، بما في ذلك تحديث أنظمة التشغيل، والبرامج والتطبيقات، ومتصفحات الويب الموجودة على الجهاز. (اللطيف، 2024)
- **تجنب الحسابات الوهمية** : بعض المحتالين ينشئون حسابات مزيفة بأسماء جهات رسمية
- **احذر الروابط المشبوهة** : إذا تلقيت رابطا يدعي تقديم مكافآت أو طلب معلومات بنكية تجنب الضغط عليه قم بالتأكيد من الجهة قبل أي إجراء.
- إدخال المعلومات الشخصية عبر المواقع الموثوقة فقط .
- الإبلاغ عن الجرائم فور حدوثها. (بن ثاني، 2019)
- يُنصَح بإبقاء المعلومات الشخصية مخفية دائماً، وتجنب مشاركتها عبر حسابات مواقع التواصل الاجتماعي؛ لأنّ ذلك قد يوفر فرصة مناسبة للمجرمين الإلكترونيين، للحصول عليها واستغلالها

للوصول إلى نواياهم الخبيثة، حيث يمكنهم مثلاً استخدام معلومات تاريخ الميلاد وبعض المعلومات الشخصية الأخرى لاختراق كلمة المرور الخاصة بالحساب. (اللطيف، 2024)

- بالإضافة إلى ذلك يجب الحرص على عدم إضافة أيّ معلومة شخصية على المواقع الإلكترونية، قبل التأكد من صحتها وأمانها، مثل تقديم أرقام الحسابات، وكلمات المرور، وما إلى ذلك.
- عدم التجاوب مع رسائل الفوز. (بن ثاني، 2019)
- **الحذر من العروض المغرية** : اذا بدا العرض جيدا جدا لدرجة لا تصدق فمن المحتمل انه احتيال احذر من الرسائل التي تعد بجواز او مبالغ مالية ضخمة.
- تجنب مشاركة الموقع المباشر. (البنك السعودي للإستثمار، 2025)
- استخدام برامج الحماية من الفيروسات. (بن ثاني، 2019)

المبحث الثالث: الثقافة الرقمية

1. تحديد المفاهيم

الثقافة لغة: ثقف الشيء، حذفته وثقفته إذا ظفرت به.

الثقافة اصطلاحا: تعرف بأنها مجموع ما يتعلم وينقل من قيم واتجاهات ومعتقدات وأفكار ترتبط بمجتمع ما من خلال تفاعل الفرد مع أسرته والبيئة المحيطة به.

الرقمية في اللغة : الرقم والترقيم تعجيم الكتاب ورقم الكتاب برقمه رقما اعجمه وبينه ويرقم في الماء اي بلغ من حذقه بالأمور أن يرقم. (حياة، 2022، صفحة 309)

اصطلاحا : عرفها الشامي بأنها عملية تحويل المواد التناظرية الي شكل الكتروني يعني رقمي وخصوصا للتخزين والاستخدام في الكمبيوتر.

أولا: تعريف الثقافة الرقمية

1. الثقافة الرقمية

مفهوم توعية الثقافة الرقمية : هي القدرة علي استخدام أجهزة الكمبيوتر والخدمات الالكترونية لمواكبة حياة المجتمعات الحديثة والمشاركة فيها بثقة ويكمن جوهرها في تمكين أفراد المجتمع من استخدام التطبيقات الرقمية الحقيقية لما لها من ثقة لإنجاز أعمالهم الوظيفية والشخصية أو واجباتهم ومهامهم اتجاه المجتمع. (حسين، 2020)

وكما يعتبر مفهوم الثقافة الرقمية : من المفاهيم الحديثة في ساحة العلوم الاجتماعية فهو يشير الي المجال الذي يرتبط به أي رقمي حيث نجد الثقافة الصحية مرتبطة بمجال الصحة والثقافة البيئية مرتبطة بمجال البيئة وغيرها أو امتلاك الفرد للسلوكيات المعرفية التي يمكن من خلالها التفاعل مع هذا المجال. (غرت، 2008)

وتعرف بأنها الحد الأدنى من المعلومات والمهارات الأساسية لدى الفرد التي يجب أن يمتلكها لتمكنه من تشغيل الحاسوب والتعامل مع برامجه واستخدام شبكة الانترنت والاستفادة منها والوعي بأخلاقيات استخدام التكنولوجيا . (حياة، 2022)

كما عرفت بأنها عملية ميكنة جميع مهام وأنشطة المؤسسات الإدارية بالاعتماد على جميع تقنيات المعلومات الضرورية للوصول إلي تحقيق أهداف الإدارة الجديدة في تقليل استخدام الورق وتبسيط الإجراءات والقضاء علي الروتين والانجاز السريع والتدقيق للمهام والمعاملات لتكون كل إدارة جاهزة لربطها بالحكومة الالكترونية لاحقا. (السماك عبد فتحي غانم، 2019، صفحة 639)

يعتبر مفهوم الثقافة الرقمية من المفاهيم الحديثة في ساحة العلوم الاجتماعية فهو يشير إلى المجال الذي يرتبط بالمجال الرقمي حيث نجد الثقافة الصحية مرتبطة بمجال الصحة الثقافة البيئية مرتبطة بمجال البيئة وتعني هذه المصطلحات التمكن من مجال معين أو امتلاك الفرد للسلوكيات المعرفية التي يستطيع من خلالها التفاعل مع هذه المجالات. (حسيبة، 2017، صفحة 67)

وحسب ما ذهب إليه السيد نجم على أنها : كل نص يتشكل بحسب معطيات التقنية الرقمية بتوظيف اللغة الرقمية والبرامج المتاحة داخل جهاز الكومبيوتر بحيث يتضمن الصورة ، الصوت ، اللون ، الحركة، الكلمة وغيرها في تشكيل فني يساعد على نمو الذوق والشخصية ويتوافق مع احتياجات عالم الطفل الشعورية والمعرفية . (سمير، 1971، صفحة 12)

الثقافة الرقمية هي امتلاك كل الوعي والقدرة على استخدام الأدوات والمرافق الرقمية بشكل مناسب لتحديدها والوصول إليها وإدارتها ودمج وتقييم وتحليل وتجميع الموارد الرقمية إنه إذن وبناء معرفة جديدة وكما اتخذ مفهوم الثقافة الرقمية عدة مصطلحات من بينها الثقافة الافتراضية ثقافة الإنترنت أو الثقافة الإلكترونية. (حسيبة، 2017، صفحة 68)

وكما ورد تعريف الثقافة الرقمية حسب الجمعية الدولية لتكنولوجيا التعليم ISTE بأنها منظمة متفاعلة من الاستراتيجيات، المعارف، المهارات، المعايير القواعد، الضوابط، الأفكار، والمبادئ المتبعة في الاستخدام الأمثل والقيم للتقنيات الرقمية واستثمارها بطريقة ذكية وآمنة من خلال التحكم فالوصول إلى المحتوي الرقمي وإنتاجه من خلال عمليات الإتاحة العادلة والتوجه نحو منافع التقنيات الحديثة والحماية من أخطارها وتعزيز المعرفة والممارسات المثلى. (فاطمة، 2019، الصفحات 420-421)

ومن المفاهيم السابقة يتضح أن الثقافة الرقمية تشير الى معارف ومهارات الفرد في إطار استخدام تكنولوجيا المعلومات، كاستخدام أجهزة الكومبيوتر والخدمات الالكترونية وتطبيقاتها وتقلباتها المتجددة، وتنمية آليات التفاعل معها ،ويكمن جوهرها في تمكين الفرد من استخدام التطبيقات الرقمية بكفاءة وثقة لإنجاز أعماله الوظيفية والشخصية المنوطة به. (رمضان محمود، 2019، صفحة 1548)

ثانيا: أهمية نشر الثقافة الرقمية وخصائصها

1. أهمية نشر الثقافة الرقمية

في ظل التطورات التكنولوجية ووسائل التواصل الحديثة والتقنيات الرقمية فان الأمر يتطلب ثقافة بمعارف ومهارات حول استخدام الأجهزة والوسائل الالكترونية والتطبيقات وتكوين ضوابط ومهارات ذاتية تمكنه من التلقي والتفاعل مع الفيض الالكتروني والرقمي بما يساعد على حسن الانتقاء والتفاعل السليم والأمن.

تكوين خلفية معرفية وأدائية عن التعامل الرقمي والالكتروني في كل مجالات الحياة فبدون تلك الثقافة لا يستطيع الإنسان أن يتواصل الكترونيا ولا يمكنه الاستفادة من الوسائل الالكترونية الضرورية وقد يقع في الكثير من المشكلات حال استخدامه تعاملات رقمية بدون توفر ثقافة رقمية مرتبطة بتلك التعاملات. (الملتقى الثاني للثقافة الرقمية، 2025)

الفرد المثقف رقميا هو الذي يعرف بعمق التفاعل الكوني لذالك يصبح الوعي الكوني مفتاح الثقافة الإعلامية ويتكون من ثلاث مستويات :

مهارات استخدام تقنيات المعلومات وتصفح الشبكات الرقمية وهو ما يجب تنميتها لطلاب وما يرتبط بتنمية المواطنة الرقمية.

مهارات التفكير الناقد لمحتوي الرسائل الإعلامية والرقمية .

تمكين الأفراد: تساعد الثقافة الرقمية الأفراد على اكتساب المهارات اللازمة لاستخدام التكنولوجيا بشكل فعال ومسئول، مما يمكنهم من الوصول إلى فرص التعليم والعمل والمعلومات.

الاستدامة الاجتماعية: الثقافة الرقمية تساعد في سد الفجوة الرقمية بين الأفراد والمجتمعات، مما يضمن مشاركة الجميع في الحياة الرقمية . (كامل)

التعلم والتطوير: كما تساعد على تطوير المهارات الرقمية ، مما يتيح للأفراد مواكبة التطورات التكنولوجية والتعلم المستمر .(Michael, 2023)

التحول الرقمي: الثقافة الرقمية هي العامل الأساسي في عملية التحول الرقمي ، وهي ضرورية لتبني التكنولوجيا الجديدة ودمجها في حياتنا . (كامل)

الابتكار: الثقافة الرقمية تشجع الابتكار والإبداع ،مما يساعد في تطوير منتجات وخدمات جديدة . (is a Digetal Coultoure and why is it important ?, 2024)

تطوير الخدمات: تساهم كذلك في تطوير الخدمات الحكومية والخاصة، مما يجعلها أكثر كفاءة وفعالية . (كامل)

تيسير الوصول إلي المعلومات: تساعد في وصول إلي المعلومات والمعرفة بسهولة .مما يجعل الأفراد أكثر وعيا .(Michael, 2023)

تعزز الثقافة الرقمية من فعالية البنية الثقافية والتعليمية وتحفز الجهات المعنية بذالك (مدارس، جامعات ، منظمات ، المجتمع المدني ، مؤسسات .....الخ لكي تسهم في تأمين تنمية الثقافة الرقمية أي العمل على الحساب والخبرات والمهارات وإعطاء فرص ومجالات تعليمية مناسبة. (حياة، 2022، صفحة 312)

المرونة: الثقافة الرقمية تجعل الأفراد والمنظمات أكثر مرونة في مواجهة التحديات والتغيرات .

تعزيز المشاركة المدنية: تساهم في تعزيز المشاركة المدنية والاجتماعية ، مما يجعل الأفراد أكثر وعيا بدورهم في المجتمع .(Michael, 2023)

تطوير المهارات الحياتية: تساهم في تطوير المهارات لدى الأفراد وذالك بتطوير التفكير النقدي وحل المشكلات.

2. خصائص الثقافة الرقمية

لقد برز لدى الثقافة الرقمية مجموعة من الخصائص من أهم هاته الخصائص نذكر:

- **محو الأمية الرقمية:** وهذا ينطوي على استخدام وسائل الإعلام والاتصال الجديدة لتقييم وفرز المعلومات.
- **الاستمرارية و الترابط:** فكل ما نقوم به في العالم الريفي يترك أثرا طويل المدى وهذا ما يخلق فرصة للوصول المستمر للبيانات والمعلومات.
- **القابلية للنسخ** : يمكن استنساخ المعلومات والمنتجات الرقمية بكل سهولة.
- **اللحظية:** إذ نقوم بإرسال واستقبال المعلومات وبطريقة فورية في البيئة الرقمية.
- **الهوية:** نستخدم عروض الثقافة المعاد خلطها رقميا لبناء الهوية وتفتح مجالا للإبداع والابتكار.
- **تعدد المهام** : هذا يعني انه يتم ادارة العديد من المهام في الوقت الملائم لذلك. (حياة، 2022، صفحة 311)

ثالثا:أهم إستراتيجيات نشر الثقافة الرقمية و اكتسابها

1. أهم استراتيجيات نشر الثقافية الرقمية

يتطلب تطوير الثقافة الرقمية استراتيجيات شاملة تشمل هاته الاستراتيجيات:

تطوير البنية التحتية التكنولوجية : يجب التركيز علي توسيع نطاق الوصول إلى الانترنت والأجهزة الرقمية ، وزيادة سرعتها وجودتها لضمان وصول أكبر عدد ممكن من الأفراد إلى الأدوات والوسائل الرقمية لازمة. (استراتيجية ورش عمل لثقافة الرقمية، 2024)

توفير برامج تعليمية وورش عمل : يجب تقديم برامج تعليمية وورش عمل موجهة لجميع الفئات العمرية ، لتنمية المهارات الرقمية الأساسية ، مثل استخدام الانترنت ،وادارة الملفات ، وانشاء العروض التقديمية. (استراتيجية ورش عمل لثقافة الرقمية، 2024)

تشجيع المؤسسات على تبني مناهج وأنشطة رقمية : يجب تشجيع المؤسسات التعليمية والثقافية على تطوير مناهج رقمية ، وتنظيم أنشطة رقمية تهدف إلى نشر الوعي بأهمية التقنيات الرقمية وكيفية الاستفادة منها . (استراتيجية ورش عمل لثقافة الرقمية، 2024)

إشراك القطاع الخاص والمجتمع المدني : لابد من تشجيع القطاعين المساهمة في جهود تطوير الثقافة الرقمية من خلال تقديم برامج وخدمات رقمية ، ودعم المبادرات التعليمية وتوفير فرص عمل في مجال التكنولوجيا . (استراتيجية ورش عمل لثقافة الرقمية، 2024)

توعية المجتمع بأهمية الثقافة الرقمية : يجب تنظيم حملات توعية لجميع فئات المجتمع حول أهمية الثقافة الرقمية ، وتأثيرها الايجابي على جميع جوانب الحياة ، مثل العمل ، والتعليم ، والتواصل الاجتماعي . (فاطمة، 2019)

تطوير المهارات الرقمية النقدية : يجب التركيز على المهارات النقدية في التعامل مع المحتوى الرقمي ، مثل التفكير النقدي وتحليل المعلومات ، وتقدير مصادر المعلومات . (استراتيجية ورش عمل لثقافة الرقمية، 2024)

تعزيز الابتكار الرقمي : يجب تشجيع الابتكار الرقمي في مختلف المجالات ،مثل التعليم ،العمل ،والخدمات العامة وتقديم الدعم الازم للمبتكرين الرقميين .

تعزيز التواصل الفعال في البيئة الرقمية : يجب التركيز على تطوير مهارات التواصل الفعال في البيئة الرقمية ، مثل استخدام أدوات التواصل الرقمي المختلفة ،والتعامل مع المعلومات الرقمية بشكل فعال .

توفير حماية الأمن السيبراني : يجب توعية الأفراد بضرورة حماية أمنهم السيبراني ،وتوفير أدوات ووسائل حماية مناسبة للحد من المخاطر الرقمية . (المدونة العربية لتنمية الإدارية الملتقى العربي الأول لتحول الرقمي "دور واهمية الثقافة الرقمية في تعزيز سياسات التحول الرقمي ": الفرص والتحديات، 2024)

تعزيز دور المكتبات العامة: لابد من تعزيز دور المكتبات العامة في نشر الثقافة الرقمية من خلال تنظيم فعاليات وورش عمل رقمية ،وتوفير خدمات رقمية متنوعة . (فاطمة، 2019)

رابعا: العلاقة بين الثقافة الرقمية والاحتيال الالكتروني

1. اثر الثقافة الرقمية للوقاية من الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي

تعد العلاقة بين الثقافة الرقمية والاحتيال الالكتروني علاقة عكسية وذالك بسبب تأثر كل واحدة بالأخرى وتعد العلاقة القائمة بينهم علاقة عكسية ، فكلما كانت نسبة الثقافة الرقمية مرتفعة قلة نسبة الاحتيال الالكتروني والعكس صحيح ، فنجد الأفراد الذين يمتلكون نسبة ثقافة رقمية مرتفعة لديهم أفضل الأساليب لتجنب وكشف عمليات الاحتيال الالكتروني.

كما تعد الثقافة الرقمية ركنا أساسيا في الوقاية من الاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي فهي تمنح المستخدمين القدرة على التعرف على أساليب الاحتيال وامكانية التصرف بوعي وثقة في البيئة الرقمية . (طارق محمد، 2022، صفحة 310)

إن الثقافة الرقمية مهارة تتطور مع مرور الوقت . كما تساهم الثقافة الرقمية في ادراك المستخدمين لأساليب الاحتيال المختلفة ، مثل التصيد الاحتيالي وانتحال الشخصية مما يساعدهم هذا على تجنب الوقوع ضحية لعمليات الاحتيال الالكتروني . (دليل الاحتيال عبر مواقع التواصل الاجتماعي ، ماهي عمليات الاحتيال على وسائل التواصل الاجتماعي ؟, مركز استشارات ادارة الأموال عبر الانترنت)

تعد الثقافة الرقمية مهارة أساسية للأفراد لتحقيق القدرة التنافسية، ولا يمكن إلا لمن يتمتعون بمهارات وثقافة رقمية معينة استكشاف قيم البيانات بشكل أفضل والاستمتاع بالخدمات الرقمية. (Du، 2024، الصفحات 377-364)

وكما يجب ترقية الثقافة الرقمية لدى المجتمع من خلال تكثيف الحصص والبرامج التي تشرح مخاطر التوظيف السيئ للتكنولوجيا على الأفراد والأطفال خصوصا ، وأساليب التحايل الرقمي في شتى الميادين : التجارة والأموال ، الابتزاز، انتحال الشخصية ،التشهير ،القرصنة ، الاختراق ، مع تقديم

إرشادات هامة حول الإجراءات اللازم اتخاذها للوقاية منها أو تدابير الحماية حال التعرض لمثل هذه الحالات . (لخضر، 2020)

الثقافة الرقمية باعتبارها القدرة على اكتساب المعلومات ومعالجتها وتقييمها في البيئة الرقمية، تلعب دورا حيويا في الحد من تعرض السكان لخسائر الاحتيال، وذلك للأسباب التالية بشكل رئيسي.

كما تنمى الثقافة الرقمية المحسنة القدرة المعرفية للأفراد على تحديد التهديدات والمخاطر المحتملة في البيئة الرقمية ، يميل السكان ذوو الثقافة الرقمية الأعلى إلى التفكير بشكل أكثر . (Du، 2024)

الفصل الثالث

الإطار التطبيقي للدراسة

خطـــــــــة الدراســـــــة(الفصل الثالث)

أولا:الأساليب الإحصائية المستخدمة

ثانيا: تحليل البيانات الشخصية

ثالثا: تحليل محاور وأسئلة الدراسة

رابعا: النتائج والاستنتاجات

اولا: تحليل البيانات الشخصية

1. الجنس:

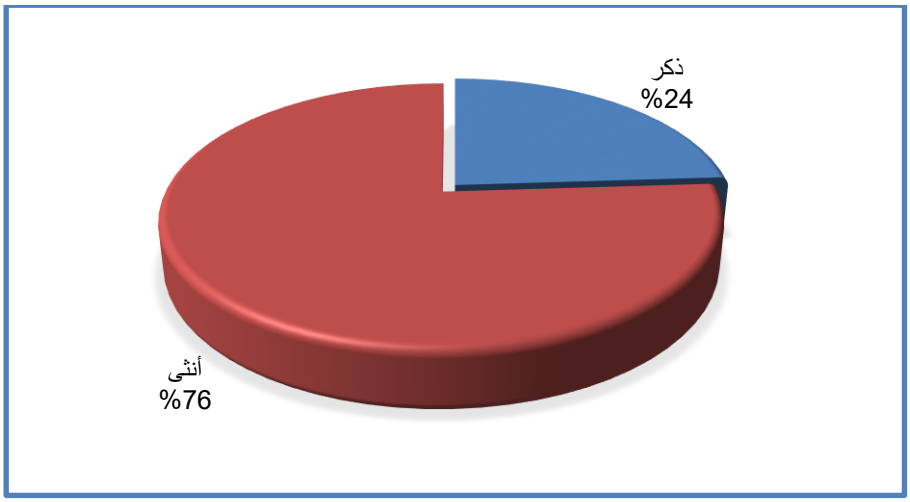
الجدول 2: توزيع أفراد العينة حسب خاصية الجنس

المتغير	التكرارات	النسبة المئوية
ذكر	24	%24
أنثى	76	%76
المجموع	100	%100

يتضح أن غالبية أفراد العينة من الإناث بنسبة 76%، مقابل 24% من الذكور. هذا التفاوت الكبير في التوزيع يشير إلى أن النساء أكثر تفاعلاً مع الاستبيان وأنهن أكثر حضورًا في الفضاء الرقمي الذي نُشر فيها الاستبيان. كما هو مؤشر على أن النساء أكثر تعرضًا أو اهتمامًا بموضوع الاحتيال الإلكتروني مما جعلهن أكثر استعدادًا للمشاركة.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب خاصية الجنس



2. السن:

الجدول 3: توزيع أفراد العينة حسب خاصية السن

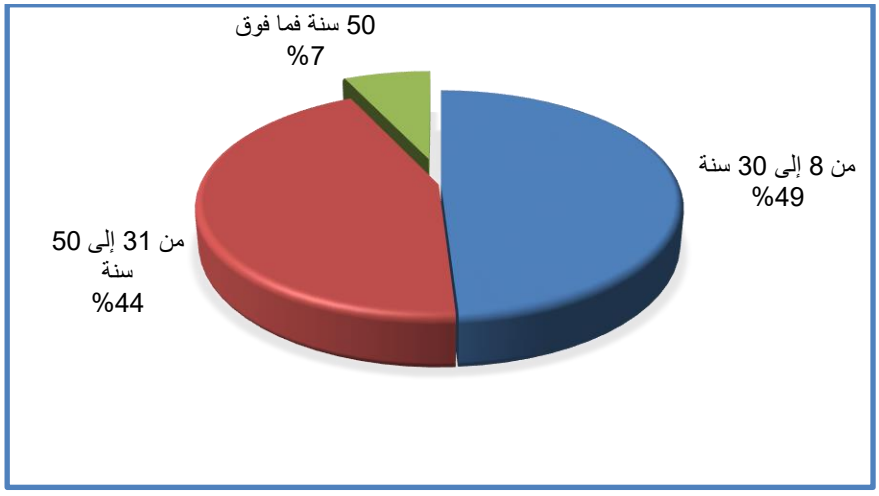
المتغير	التكرارات	النسبة المئوية
من 8 إلى 30 سنة	49	%49
من 31 إلى 50 سنة	44	%44
50 سنة فما فوق	7	%7
المجموع	100	%100

تشير النتائج إلى أن الفئة الشابة (من 8 إلى 30 سنة) تمثل النسبة الأكبر (49%)، تليها الفئة المتوسطة (31 إلى 50 سنة) بنسبة 44% .

هذه الأرقام تعكس الطابع العام لمستخدمي مواقع التواصل الاجتماعي، حيث تُمثل الفئتان الأصغر سنًا غالبية المستخدمين النشطين، وبالتالي الأكثر عرضة للتفاعل مع المحتوى الاحتيالي. أما الفئة التي تفوق 50 سنة فتمثل نسبة ضئيلة (7%)، وهو أمر متوقع نظرا لقلة استخدامهم لمواقع التواصل مقارنة بالفئات الأخرى.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب خاصية السن



3. المستوى التعليمي:

الجدول 4: توزيع أفراد العينة حسب خاصية المستوى التعليمي

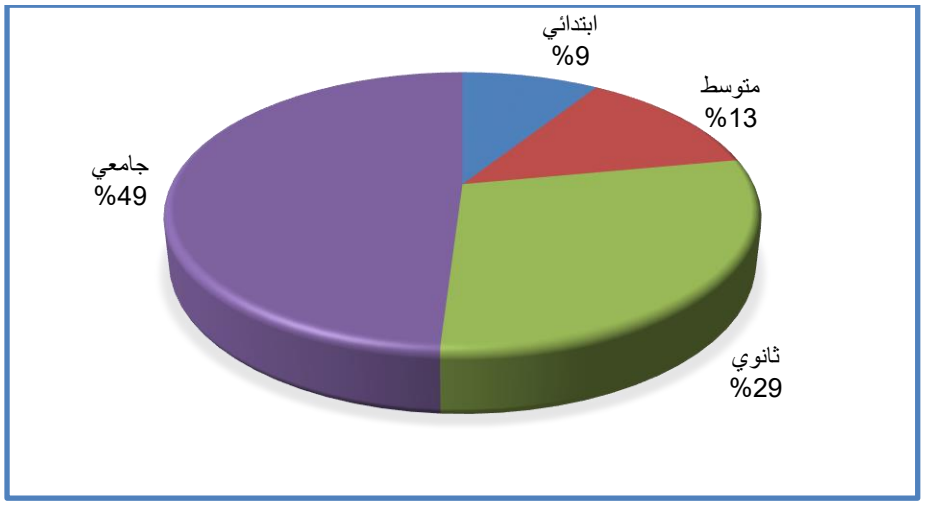
المتغير	التكرارات	النسبة المئوية
ابتدائي	9	%9
متوسط	13	%13
ثانوي	29	%29
جامعي	49	%49
المجموع	100	%100

يشير التوزيع إلى أن الأفراد ذوي المستوى الجامعي يُشكّلون النسبة الأكبر (49%)، يليهم الحاصلون على التعليم الثانوي(29%) .

هذا التوزيع قد يكون مرتبطًا بطبيعة الأفراد الذين لديهم قدرة أكبر على فهم الاستبيانات والمشاركة في الدراسات الأكاديمية. لكن من ناحية موضوع الدراسة فإن ارتفاع المستوى التعليمي لا يمنع من التعرض للاحتيال الإلكتروني، بل أحيانًا قد يُستهدف المتعلمون بأساليب احتيالية أكثر تطورًا.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب خاصية المستوى التعليمي



4. عدد ساعات استخدام مواقع التواصل الاجتماعي يوميا:

الجدول 5: توزيع أفراد العينة حسب خاصية عدد ساعات استخدام مواقع التواصل الاجتماعي

المتغير	التكرارات	النسبة المئوية
أقل من ساعة واحدة	5	5
من 1 إلى 4 ساعات	25	25
من 4 إلى 6 ساعات	38	38
أكثر من 6 ساعات	32	32
المجموع	100	100

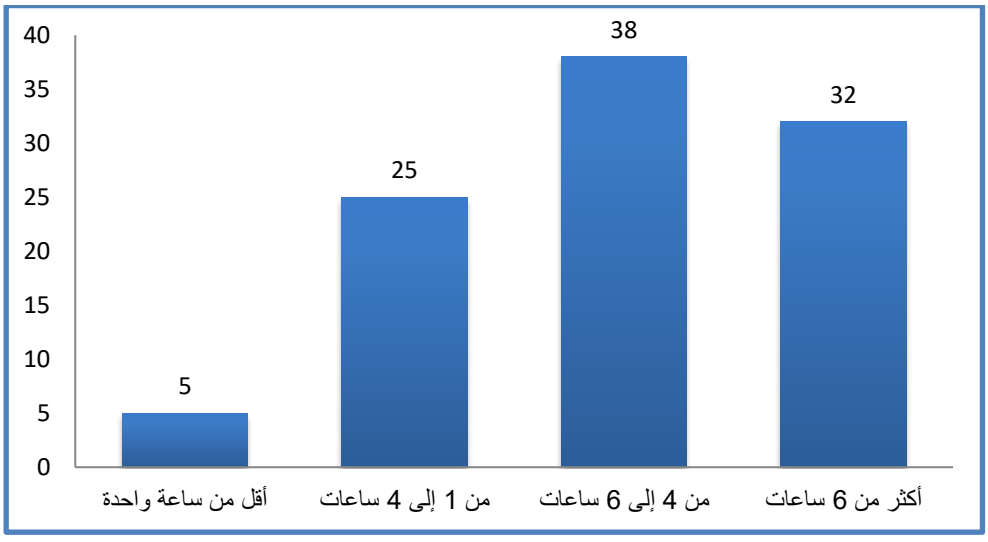
تشير النتائج إلى أن 70%من العينة يستخدمون مواقع التواصل الاجتماعي لأكثر من 4 ساعات يوميًا، وهو رقم مرتفع نسبيًا ويُبرز درجة التعرض المستمر والمتكرر للمحتوى الرقمي.

كلما زادت ساعات الاستخدام زادت فرص التعرض لمحاولات الاحتيال الإلكتروني خاصة عبر الإعلانات، الروابط المشبوهة والرسائل الخاصة.

هذا المعطى مهم جدًا لأنه يعزز الفرضية التي تفيد بأن الاستعمال المكثف لمواقع التواصل يجعل الأفراد أكثر عرضة للوقوع في فخ الاحتيال الإلكتروني.

والشكل الموالي يوضح ذلك:

توزيع أفراد **العينة** حسب خاصية عدد ساعات استخدام مواقع التواصل الاجتماعي



ثالثا: تحليل محاور وأسئلة الدراسة

1. هل سبق أن تعرضت لعملية احتيال إلكتروني عبر مواقع التواصل الاجتماعي؟

الجدول 6: توزيع افراد العينة حسب إذا سبق تعرضهم لعملية احتيال الكتروني

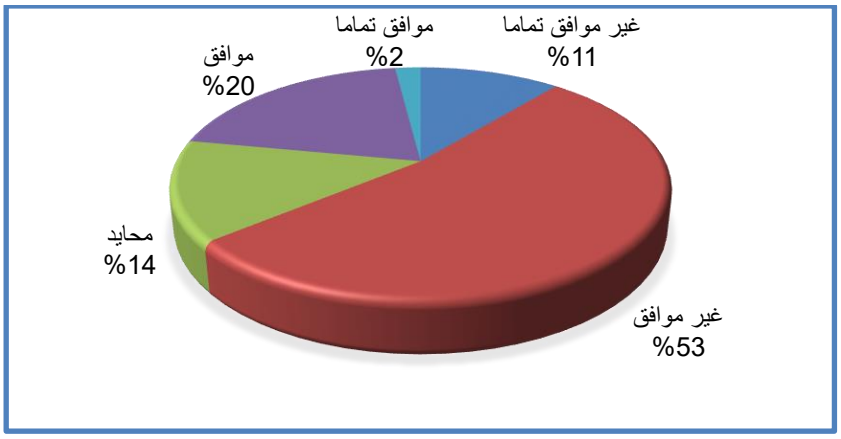
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	11	%11
غير موافق	53	%53
محايد	14	%14
موافق	20	%20
موافق تماما	2	%2
المجموع	100	%100

من خلال النتائج يتبين أن نسبة المبحوثين الذين لم يسبق لهم التعرض للاحتيال الإلكتروني بلغت 64% (11% غير موافق تمامًا، 53% غير موافق)، في حين بلغت نسبة الذين أكدوا تعرضهم له 22% (20% موافق، 2% موافق تمامًا)، بينما بقي 14% محايدين.

هذا يشير إلى أن غالبية الأفراد لم يتعرضوا بشكل مباشر للاحتيال عبر مواقع التواصل الاجتماعي، وهو ما قد يُعزى إلى وعي نسبي أو إلى محدودية تفاعلهم مع المحتويات الاحتيالية. كما يمكن تفسير انخفاض نسبة المعرضين فعلًا إما بعدم إدراك بعضهم لكونهم تعرضوا لعملية احتيال أو بسبب تحفظهم عن الإقرار بها لأسباب اجتماعية أو نفسية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب إذا سبق تعرضهم لعملية احتيال الكتروني



2. هل تعرف شخصا تعرض للاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي؟

الجدول 7: توزيع أفراد العينة حسب معرفتهم بأشخاص تعرضوا لاحتيال الكتروني

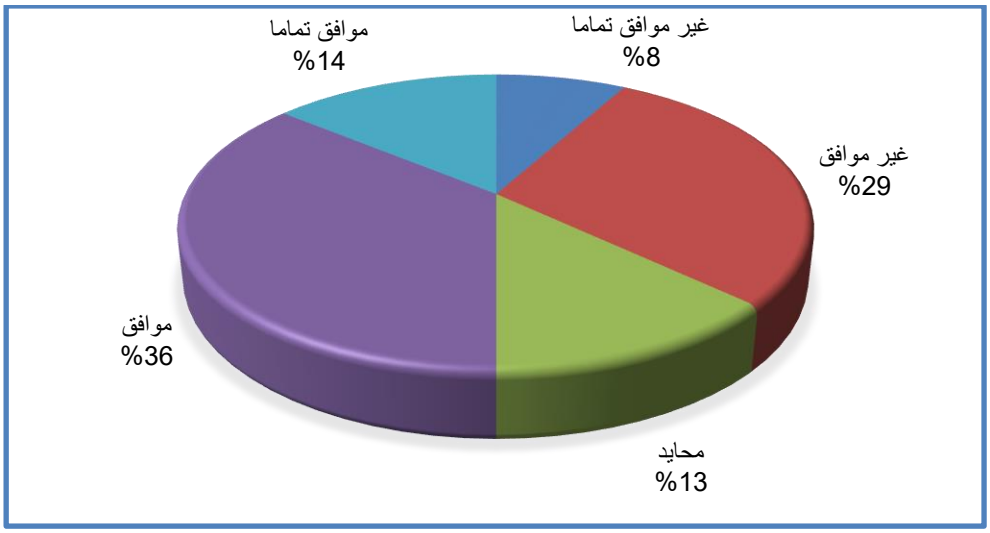
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	8	%8
غير موافق	29	%29
محايد	13	%13
موافق	36	%36
موافق تماما	14	%14
المجموع	100	%100

تبيّن النتائج أن نصف العينة (50%) صرّحوا بمعرفتهم لأشخاص تعرّضوا للاحتيال الإلكتروني، بينما نفى ذلك 37%، واحتفظ 13% بموقف محايد.

ويُفهم من ذلك أن ظاهرة الاحتيال الإلكتروني منتشرة في الأوساط الاجتماعية المحيطة بالمبحوثين، حتى وإن لم يكونوا ضحايا مباشرين لها، ما يعكس واقعًا ميدانيًا يجب أخذه بعين الاعتبار في تحليل تأثير الظاهرة.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب معرفتهم بأشخاص تعرضوا لاحتيال الكتروني



3. **هل تصلك رسائل أو روابط مشبوهة بشكل متكرر؟**

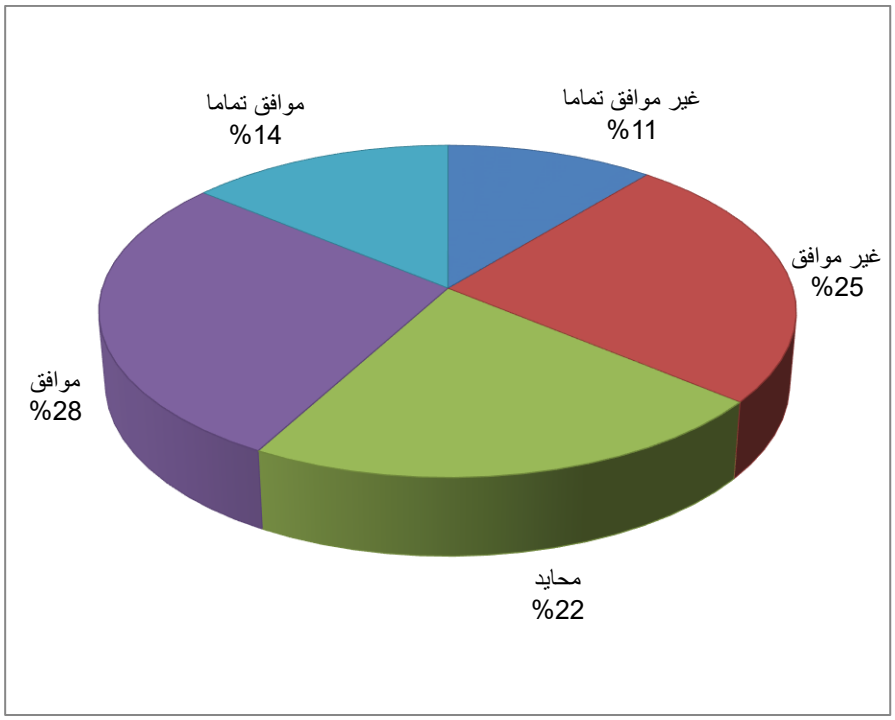
الجدول 8: توزيع أفراد العينة حسب إذا تصلهم رسائل أو روابط مشبوهة

المتغير	التكرارات	النسبة المئوية
غير موافق تماما	11	%11
غير موافق	25	%25
محايد	22	%22
موافق	28	%28
موافق تماما	14	%14
المجموع	100	%100

توضح نتائج الاستبيان أن 42% من أفراد العينة يتلقون بشكل متكرر رسائل أو روابط مشبوهة (28% موافق، 14% موافق تمامًا)، وهي نسبة مرتفعة تدل على وجود استهداف فعلي ومستمر للمستخدمين عبر وسائل التواصل. في المقابل، 36% نفوا ذلك، و22% كانوا محايدين.

تُبرز هذه النتائج خطورة البيئة الرقمية التي يتنقل فيها المستخدمون، خاصة أولئك المرتبطين بأنشطة بيع إلكتروني، ما يجعلهم هدفًا مباشرًا لعمليات احتيال ممنهجة.والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب إذا تصلهم رسائل أو روابط مشبوهة



4. هل تشعر بالقلق من الوقوع ضحية للاحتيال الإلكتروني؟

الجدول 9: توزيع أفراد العينة حسب مدى شعورهم بالقلق من الوقوع ضحية للاحتيال الإلكتروني

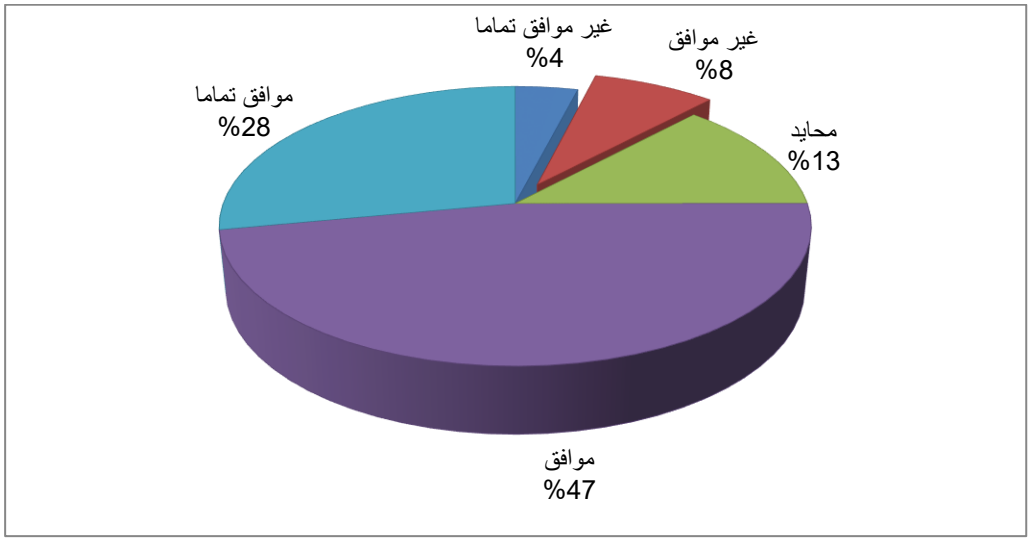
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	4	%4
غير موافق	8	%8
محايد	13	%13
موافق	47	%47
موافق تماما	28	%28
المجموع	100	%100

أظهرت النتائج أن نسبة 75% من المبحوثين يشعرون بالقلق من الوقوع ضحية للاحتيال الإلكتروني (47% موافق، 28% موافق تمامًا)، في حين أظهر 12% عدم قلقهم، و13% بقوا في منطقة الحياد.

يدل هذا على أن الإحساس بالخطر الإلكتروني مرتفع بشكل كبير لدى المستخدمين، وهو ما يمكن اعتباره مؤشرًا إيجابيًا من ناحية الوعي، غير أنه في حال لم يقترن هذا القلق بتصرفات وقائية، فإنه يظل غير كافٍ للوقاية الفعلية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب مدى شعورهم بالقلق من الوقوع ضحية للاحتيال الإلكتروني



5. هل تجد صعوبة في التمييز بين الصفحات الحقيقية والمزيفة؟

الجدول 10: توزيع أفراد العينة حسب مدى صعوبة التمييز بين الصفحات الحقيقة والمزيفة

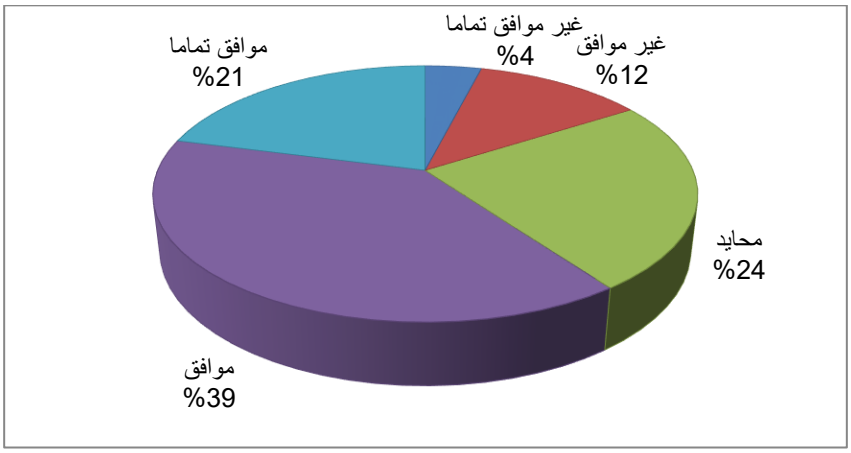
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	4	%4
غير موافق	12	%12
محايد	24	%24
موافق	39	%39
موافق تماما	21	%21
المجموع	100	%100

أفاد 60% من أفراد العينة بأنهم يواجهون صعوبة في التمييز بين الصفحات الحقيقية والمزيفة (39% موافق، 21% موافق تمامًا)، مقابل 16% فقط أنكروا وجود هذه الصعوبة، بينما بقي 24% محايدين.

ويشير ذلك إلى وجود ضعف في المهارات التقنية الأساسية لدى المستخدمين، رغم انخراطهم في بيئات رقمية تتطلب قدرًا من الحذر، مثل صفحات البيع الإلكتروني. هذه الفجوة في المهارة قد تسهّل على المحتالين تنفيذ عملياتهم.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب مدى صعوبة التمييز بين الصفحات الحقيقة والمزيفة



6. هل تعرف كيف تحمي حساباتك على مواقع التواصل الاجتماعي؟

الجدول 11: توزيع أفراد العينة حسب طريقة حمايتهم لحساباتهم على مواقع التواصل

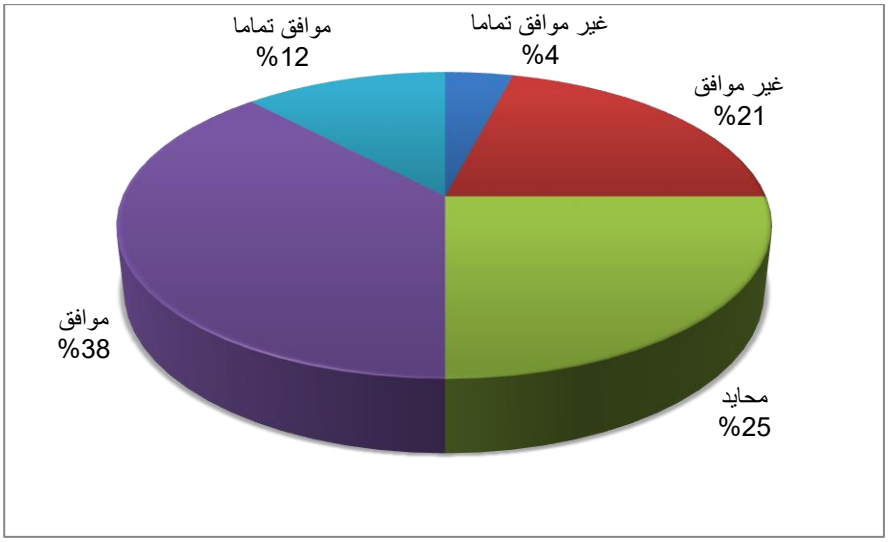
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	4	%4
غير موافق	21	%21
محايد	25	%25
موافق	38	%38
موافق تماما	12	%12
المجموع	100	%100

أظهر 50% من المبحوثين معرفتهم بكيفية حماية حساباتهم، بينما عبّر 25% عن عدم معرفتهم، و25% حافظوا على موقف محايد.

هذه النتيجة تشير إلى وجود وعي نسبي بالحماية الإلكترونية لدى نصف العينة، لكنها تؤكد في المقابل أن نصف المستخدمين الآخرين إما يفتقرون للمعرفة أو غير واثقين من إجراءاتهم، مما يعرضهم لمخاطر أكبر في الفضاء الرقمي.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب طريقة حمايتهم لحساباتهم على مواقع التواصل



7. هل تفعل خاصية التحقق بخطوتين لحساباتك الشخصية؟

الجدول 12: توزيع أفراد العينة حسب مدى تفعيلهم لخاصية التحقق من الحساب الشخصي

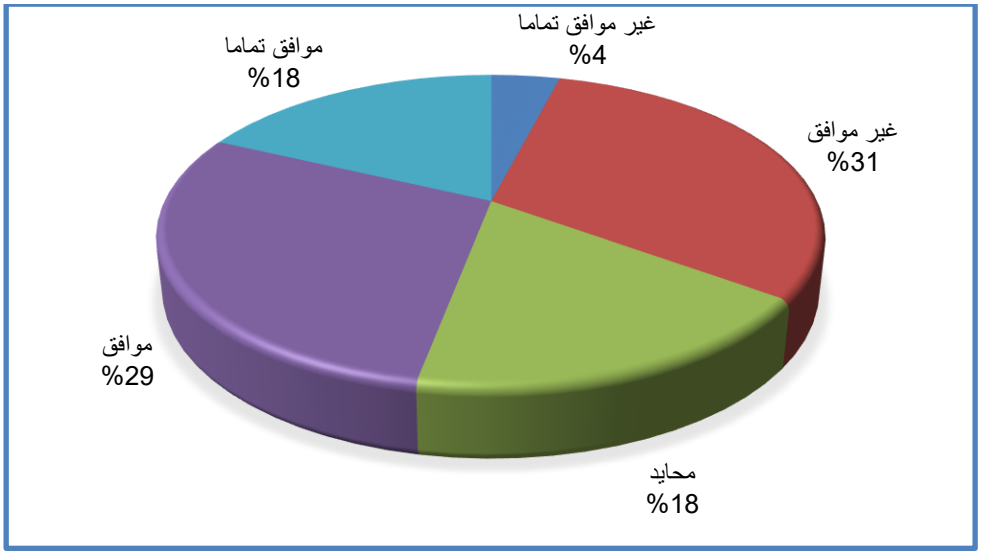
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	4	%4
غير موافق	31	%31
محايد	18	%18
موافق	29	%29
موافق تماما	18	%18
المجموع	100	%100

من خلال النتائج الموضحة في الجدول السابق نجد أن 47% من الأفراد فقط يقومون بتفعيل هذه الخاصية الأمنية (29% موافق، 18% موافق تمامًا)، بينما عبّر 35% عن عدم تفعيلهم لها، و18% كانوا محايدين.

تعكس هذه النتيجة ضعف التطبيق العملي للثقافة الرقمية، فبالرغم من معرفة الكثيرين بأهمية الحماية، إلا أن قلة فقط تعتمد أدوات أمان متقدمة، مثل التحقق الثنائي.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب مدى تفعيلهم لخاصية التحقق من الحساب الشخصي



8. هل تنقر على روابط من مصادر غير موثوقة؟

الجدول 13: توزيع أفراد العينة حسب مدى نقرهم على الروابط غير الموثوقة

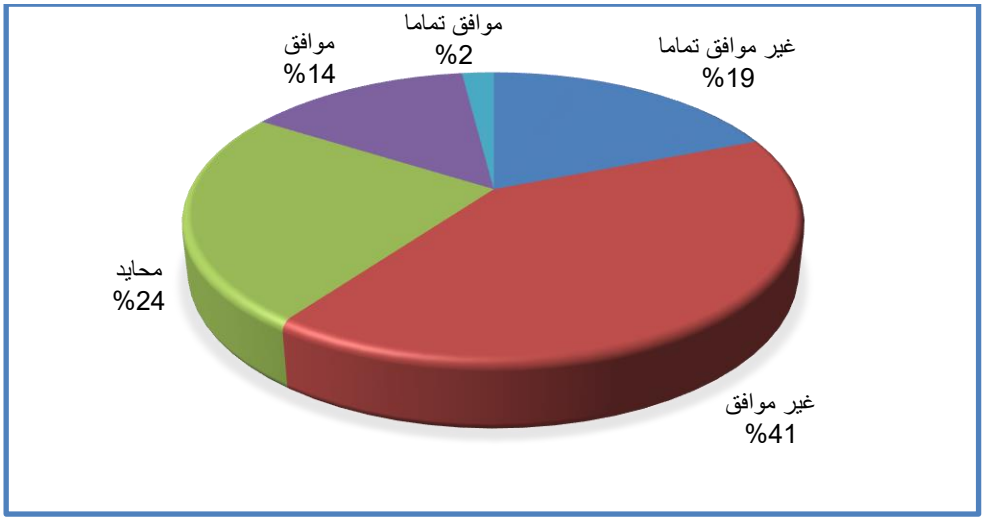
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	19	%19
غير موافق	41	%41
محايد	24	%24
موافق	14	%14
موافق تماما	2	%2
المجموع	100	%100

من خلال الجدول السابق نجد أن نحو 60% من العينة لا ينقرون على روابط مشبوهة (41% غير موافق، 19% غير موافق تمامًا)، وهو سلوك يُعد إيجابيًا، في حين أقر 16% بأنهم ينقرون على روابط من مصادر غير موثوقة، وهي نسبة مقلقة.

يعكس هذا وجود سلوك وقائي لدى غالبية العينة، لكن لا تزال هناك فئة مهددة بالفعل بسبب تهاونها في التعامل مع الروابط الرقمية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب مدى نقرهم على الروابط غير الموثوقة



9. هل تستطيع التحقق من الصفحات الرسمية بسهولة؟

الجدول 14: توزيع أفراد العينة حسب سهولة تحققهم من الصفحات الرسمية بسهولة

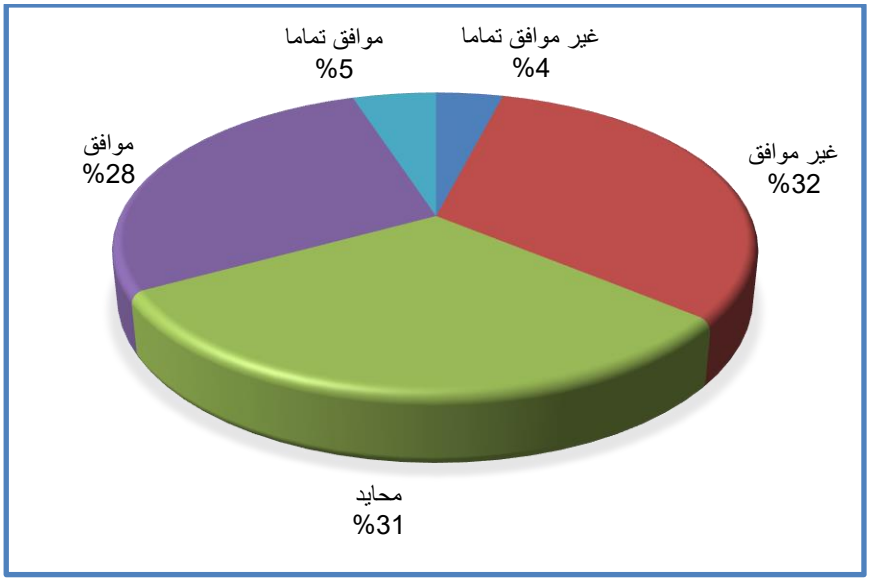
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	4	%4
غير موافق	32	%32
محايد	31	%31
موافق	28	%28
موافق تماما	5	%5
المجموع	100	%100

توضح نتائج الجدول السابق أن 33% فقط أكدوا قدرتهم على التحقق (28% موافق، 5% موافق تمامًا)، بينما 63% إما غير قادرين أو محايدين.

تُظهر هذه النتيجة قصورًا واضحًا في أدوات التمييز الرقمية، مما يجعل الأفراد عرضة للخداع من قبل الصفحات المزيفة، وخاصة في إطار الإعلانات التجارية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب سهولة تحققهم من الصفحات الرسمية بسهولة



10. هل تتابع محتوى متعلقا بالأمن الرقمي؟

الجدول 15: توزيع أفراد العينة حسب متابعهم لمحتويات الأمن الرقمي

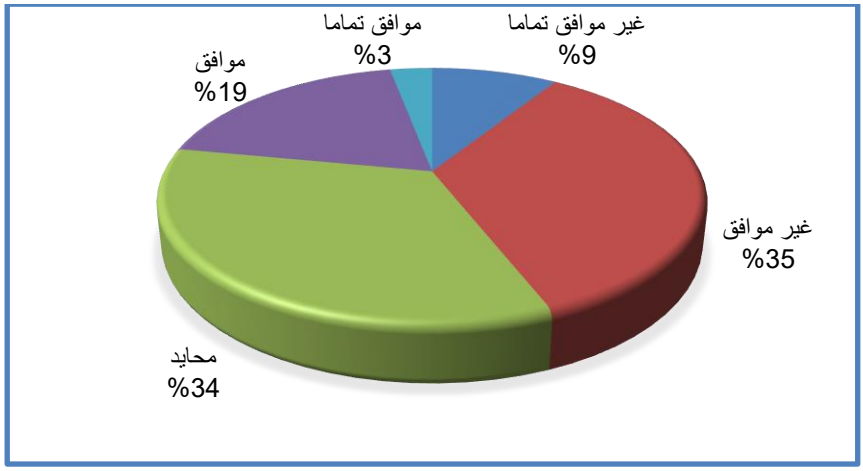
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	9	%9
غير موافق	35	%35
محايد	34	%34
موافق	19	%19
موافق تماما	3	%3
المجموع	100	%100

تشير النتائج إلى أن 22%فقط من العينة يتابعون محتوى يخص الأمن الرقمي (19% موافق، 3% موافق تمامًا)، في حين أن نسبة كبيرة تبلغ 44% صرّحت بعدم متابعتها لهذا النوع من المحتوى (35% غير موافق، 9% غير موافق تمامًا)، و34% كانوا محايدين.

هذه النسب تدل على ضعف في التفاعل المستمر مع مصادر التثقيف الرقمي، مما قد يُفسر جزئيًا غياب بعض المهارات الوقائية، رغم ارتفاع نسبة القلق من الاحتيال.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب متابعهم لمحتويات الأمن الرقمي



11. هل سبق أن شاركت في دورة أو ورشة حول الثقافة الرقمية أو الأمن الرقمي؟

الجدول 16: توزيع أفراد العينة حسب إذا سبق وشاركوا في دورات أو ورشات حول الثقافة الرقمية أو الأمن الرقمي

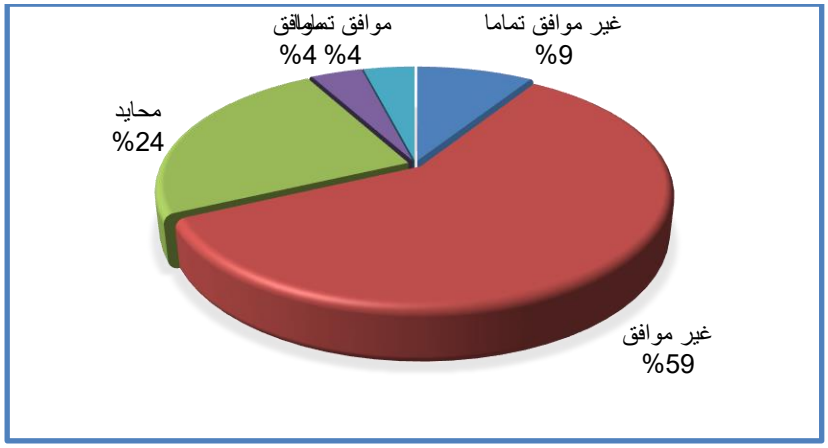
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	9	%9
غير موافق	59	%59
محايد	24	%24
موافق	4	%4
موافق تماما	4	%4
المجموع	100	%100

أظهرت النتائج أن نسبة كبيرة جدًا من المبحوثين (68%) لم يسبق لهم المشاركة في أي دورة أو ورشة تدريبية (59% غير موافق، 9% غير موافق تمامًا)، في حين لم تتجاوز نسبة من شاركوا فعليًا 8% فقط، و24% بقوا في موقف الحياد.

تعكس هذه النتيجة ضعفًا شديدًا في التكوين الرقمي الرسمي والمؤسساتي، ما يعني أن أغلب المعارف المكتسبة (إن وجدت) هي ذاتية، وقد تكون سطحية أو غير منهجية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب إذا سبق وشاركوا في دورات أو ورشات حول الثقافة الرقمية أو الأمن الرقمي



12. هل تستخدم كلمات مرور قوية لكل حساب؟

الجدول 17: توزيع أفراد العينة حسب مدى استخدامهم لكلمات مرور قوية لكل حساب

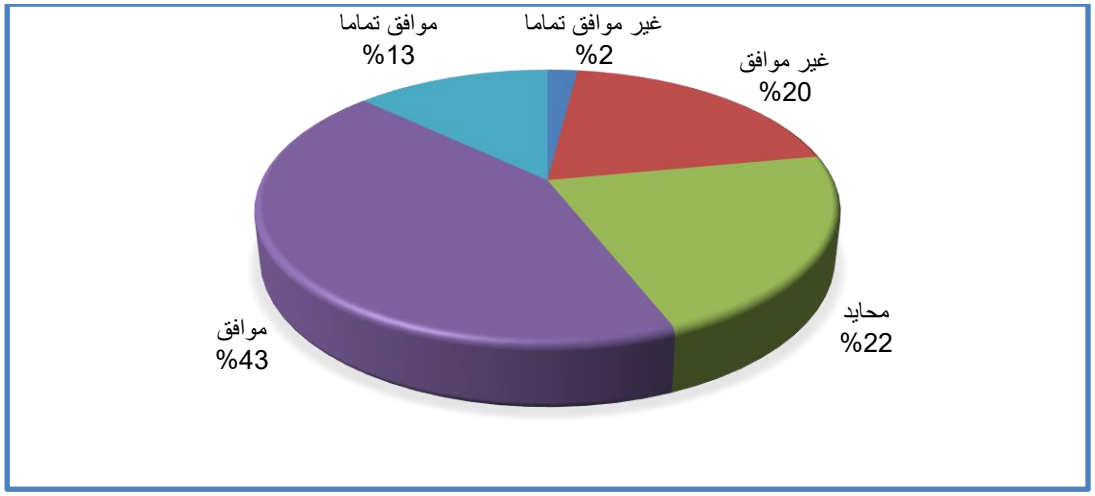
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	2	%2
غير موافق	20	%20
محايد	22	%22
موافق	43	%43
موافق تماما	13	%13
المجموع	100	%100

يتضح من النتائج أن 56%من المبحوثين يستخدمون كلمات مرور قوية (43% موافق، 13% موافق تمامًا)، في حين 22% لا يلتزمون بذلك (20% غير موافق، 2% غير موافق تمامًا)، و22% محايدين.

هذه النتيجة إيجابية نسبيًا، وتشير إلى تحسن في بعض السلوكيات الرقمية الوقائية، إلا أن بقاء ما يقارب الربع خارج إطار الأمان يشكل نقطة ضعف يجب الانتباه لها.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب مدى استخدامهم لكلمات مرور قوية لكل حساب



13. هل تراجع إعدادات الأمان في حساباتك بشكل دوري؟

الجدول 18: توزيع أفراد العينة حول مدى مراجعتهم لإعدادات الأمان شكل دوري

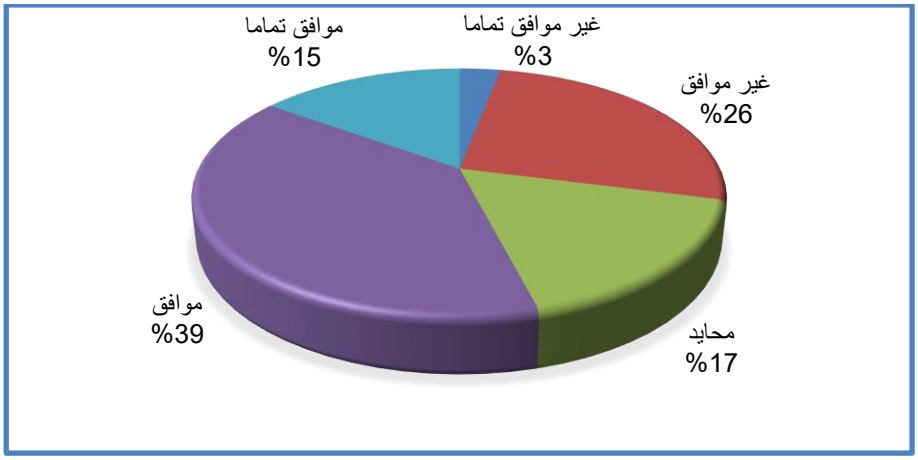
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	3	%3
غير موافق	26	%26
محايد	17	%17
موافق	39	%39
موافق تماما	15	%15
المجموع	100	%100

أفاد 54% من المبحوثين بأنهم يراجعون إعدادات الأمان بشكل دوري (39% موافق، 15% موافق تمامًا)، مقابل 29% لا يفعلون ذلك (26% غير موافق، 3% غير موافق تمامًا)، و17% محايدين.

تُظهر هذه النتيجة أن نصف العينة تقريبًا تتابع إجراءات الحماية بشكل جيد، وهو أمر مشجع، لكنه لا يزال غير كافٍ لتقليل الهجمات المحتملة ما لم يتم تعميم هذا السلوك الوقائي.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حول مدى مراجعتهم لإعدادات الأمان شكل دوري



14.هل الثقافة الرقمية تقلل من نسبة تعرضك للاحتيال الإلكتروني؟

الجدول 19: توزيع أفراد العينة حسب إذا كانت الثقافة الرقمية تقلل من نسبة تعرضهم للاحتيال

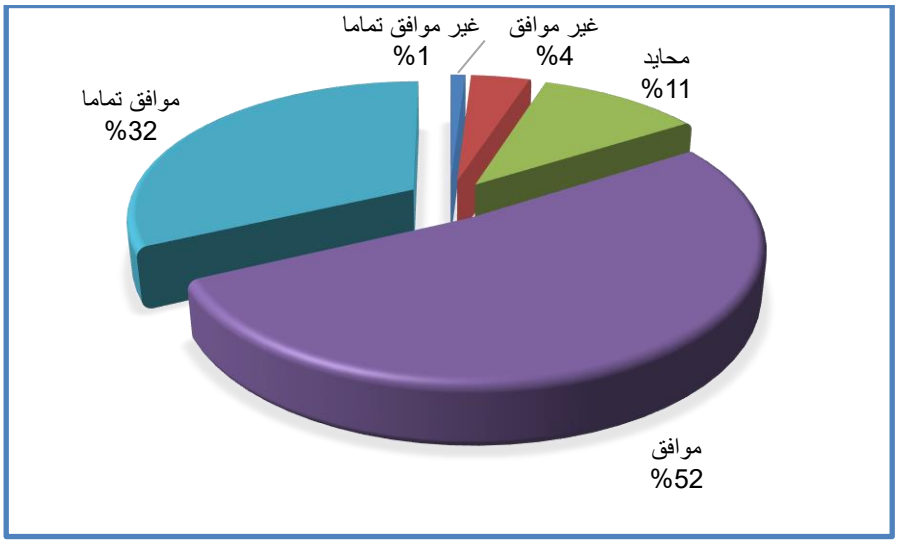
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	1	%1
غير موافق	4	%4
محايد	11	%11
موافق	52	%52
موافق تماما	32	%32
المجموع	100	%100

أظهرت النتائج أن 84%من المشاركين يعتقدون بأن الثقافة الرقمية تساهم في تقليل فرص التعرض للاحتيال (52% موافق، 32% موافق تمامًا)، مقابل 5% أنكروا ذلك، و11% كانوا محايدين.

وهذا يعكس إدراكًا عميقًا لدى العينة لأهمية الثقافة الرقمية كخط دفاع أول ضد الاحتيال الإلكتروني، ويؤكد صحة الفرضية الأساسية للدراسة.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب إذا كانت الثقافة الرقمية تقلل من نسبة تعرضهم للاحتيال



15. هل لديك ثقة في استعمال تطبيق بريدي موب لإجراء معاملاتك المالية؟

توزيع أفراد العينة حول إذا زادت المعرفة الرقمية تقل فرص التعرض للاحتيال

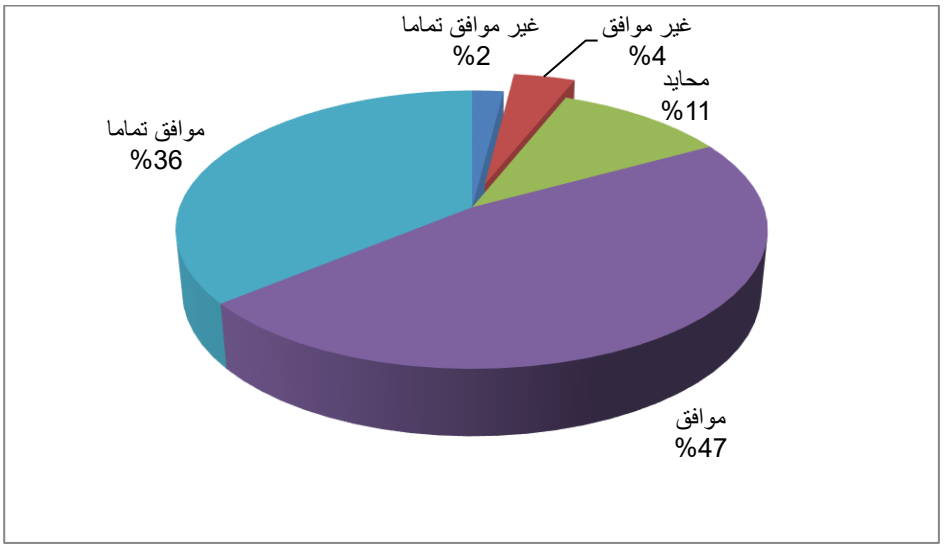
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	2	%2
غير موافق	4	%4
محايد	11	%11
موافق	47	%47
موافق تماما	36	%36
المجموع	100	%100

بيّنت النتائج أن 83% من المبحوثين يؤيدون هذا الطرح (47% موافق، 36% موافق تمامًا)، مقابل 6% غير موافقين، و11% محايدين.

وهو ما يُعزز الفرضية القائلة بوجود علاقة عكسية بين مستوى الوعي الرقمي ومخاطر التعرض للجرائم الإلكترونية، ويبرر أهمية نشر المعرفة الرقمية في أوساط المستخدمين.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حول إذا زادت المعرفة الرقمية تقل فرص التعرض للاحتيال



16. هل ضعف الثقافة الرقمة سبب رئيسي في انتشار الاحتيال الإلكتروني؟

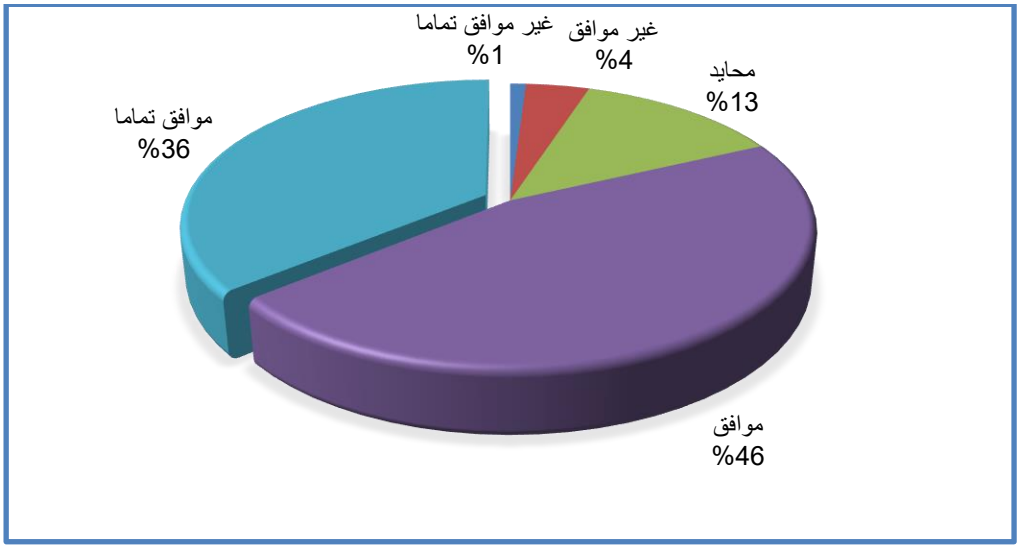
الجدول 20: توزيع أفراد العينة حول رأيهم بأن ضعف الثقافة الرقمية سبب في انتشار الاحتيال الإلكتروني

المتغير	التكرارات	النسبة المئوية
غير موافق تماما	1	%1
غير موافق	4	%4
محايد	13	%13
موافق	46	%46
موافق تماما	36	%36
المجموع	100	%100

أجاب 82% من الأفراد بالموافقة (46% موافق، 36% موافق تمامًا)، في حين رفض 5% ذلك، و13% فضلوا الحياد.

هذه النتيجة تؤكد أن العينة ترى في الجهل الرقمي أرضًا خصبة لنجاح عمليات الاحتيال الإلكتروني، ما يستوجب التدخل عبر التكوين والتوعية.

توزيع أفراد العينة حول رأيهم بأن ضعف الثقافة الرقمية سبب في انتشار الاحتيال الإلكتروني



17. هل من الضروري إدراج الثقافة الرقمية ضمن المناهج الدراسية؟

الجدول 21: توزيع أفراد العينة حسب رأيهم بأنه من الضروري إدراج الثقافة الرقمية ضمن المناهج الدراسية

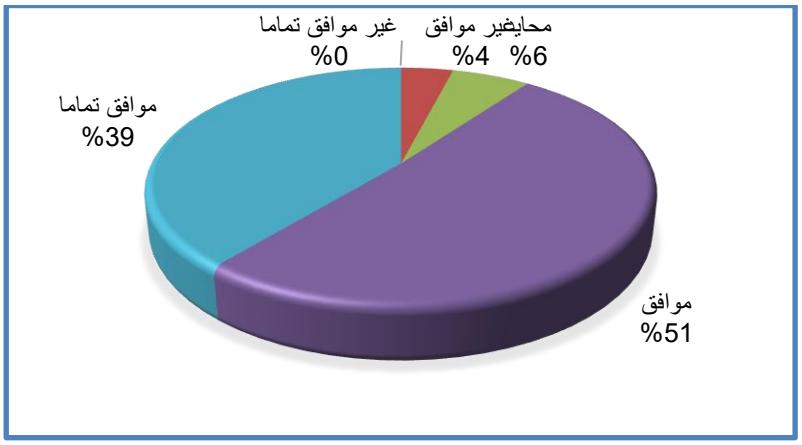
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	0	%0
غير موافق	4	%4
محايد	6	%6
موافق	51	%51
موافق تماما	39	%39
المجموع	100	%100

اتضح من النتائج أن 90% من أفراد العينة يؤيدون إدراج الثقافة الرقمية في المناهج التعليمية (51% موافق، 39% موافق تمامًا)، مقابل 4% فقط غير موافقين، و6% محايدين.

وهذا يعكس قناعة مجتمعية واسعة بأهمية التكوين المبكر في المجال الرقمي، بما يمكن المتعلمين من حماية أنفسهم مستقبلًا في الفضاء السيبراني.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب رأيهم بأنه من الضروري إدراج الثقافة الرقمية ضمن المناهج الدراسية



18. هل التوعية المجتمعية ضرورية لمواجهة جريمة الاحتيال الإلكتروني؟

الجدول 22: توزيع أفراد العينة حسب إذا كانت التوعية المجتمعية ضرورية لمواجهة جريمة الاحتيال الإلكتروني

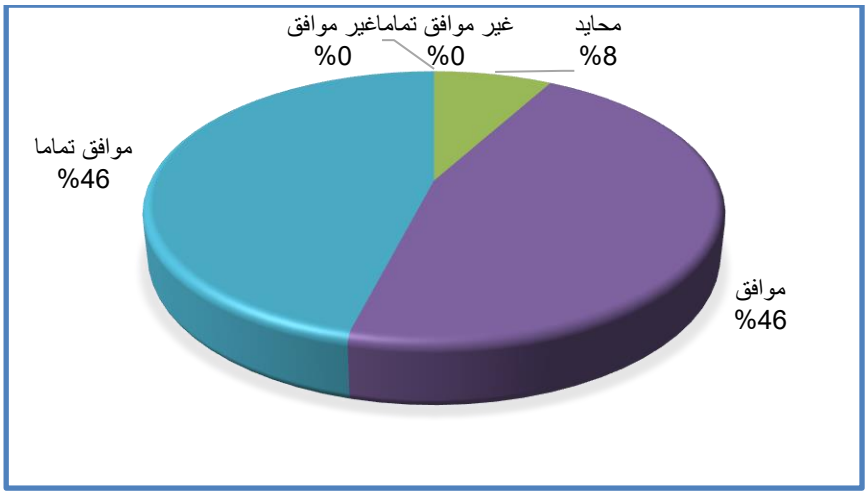
المتغير	التكرارات	النسبة المئوية
غير موافق تماما	0	%0
غير موافق	0	%0
محايد	8	%8
موافق	46	%46
موافق تماما	46	%46
المجموع	100	%100

سجل هذا السؤال أعلى نسبة تأييد في كامل الاستبيان، حيث بلغت نسبة الموافقة 92% بالتساوي بين (46% موافق و46% موافق تمامًا)، مع 8% فقط محايدين، وعدم وجود أي رفض.

ما يدل على إجماع واضح داخل العينة على أن المواجهة الفعالة لجريمة الاحتيال لا تكون فردية فقط، بل يجب أن تكون مؤسسية وشاملة عبر حملات توعية ومبادرات جماعية.

والشكل الموالي يوضح ذلك:

توزيع أفراد العينة حسب إذا كانت التوعية المجتمعية ضرورية لمواجهة جريمة الاحتيال الإلكتروني



19. هل ضعف الثقافة الرقمة سبب رئيسي في انتشار الاحتيال الإلكتروني (السن، العمر، المستوى التعليمي، عدد ساعات استخدام مواقع التواصل الاجتماعي)

الجدول 23: توزيع أفراد العينة حسب صحة الفرضية المتعلقة بأن ضعف الثقافة الرقمية سبب رئيسي في انتشار الاحتيال الإلكتروني (السن، العمر، المستوى التعليمي، عدد ساعات استخدام مواقع التواصل الاجتماعي)

			هل ضعف الثقافة الرقمة سبب رئيسي في انتشار الاحتيال الإلكتروني؟					المجموع
			غير موافق تماما	غير موافق	محايد	موافق	موافق تماما	
السن	ذكر	التكرار	0	0	2	11	11	24
		النسبة%	%0	0%	%2	%11	%11	%24
	أنثى	التكرار	1	4	11	35	25	76
		النسبة%	%1	%4	%11	%35	%25	%76
	المجموع	التكرار	1	4	13	46	36	100
		النسبة%	%1	%4	%13	%46	%36	%100

السن	من 18 إلى 30 سنة	التكرار	0	3	5	26	15	49
		النسبة%	%0	%3	%5	%26	%15	%49
	من 31 إلى 50 سنة	التكرار	1	1	7	19	16	44
		النسبة%	%1	%1	%7	%19	%16	44%
	50 سنة فما فوق	التكرار	0	0	1	1	5	7
		النسبة%	%0	%0	%1	%1	%5	%7
	المجموع	التكرار	1	4	13	46	36	100
		النسبة%	%1	%4	%13	%46	36%	%100
المستوى التعليمي	ابتدائي	التكرار	1	1	1	1	5	9
		النسبة%	%1	%1	%1	%1	%5	%9
	متوسط	التكرار	0	1	3	6	3	13
		النسبة%	%0	%1	%3	%6	%3	%13
	ثانوي	التكرار	0	1	5	17	6	29
		النسبة%	%0	%1	%5	%17	%6	%29
	جامعي	التكرار	0	1	4	22	22	49
		النسبة%	%0	%1	%4	22%	%22	%49
	المجموع	التكرار	1	4	13	46	36	100
		النسبة%	%1	%4	%13	%46	%36	%100
عدد ساعات استخدام	أقل من ساعة واحدة	التكرار	0	1	1	2	1	5
	من 1 إلى 4 ساعات	النسبة%	%0	%1	%1	%2	1%	%5

	من 4 إلى 6 ساعات	التكرار	1	0	5	10	9	25
		النسبة%	%1	%0	%5	%10	%9	%25
	أقل من ساعة واحدة من 1 إلى 4 ساعات	التكرار	0	1	6	17	14	38
		النسبة%	%0	1%	%6	17%	14%	38%
	من 4 إلى 6 ساعات	التكرار	0	2	1	17	12	32
		النسبة%	%0	%2	%1	%17	%12	32%
	المجموع	التكرار	1	4	16	46	36	100
		النسبة%	%1	%4	%16	%46	%36	%100

نلاحظ من خلال الجدول السابق وجود تباين واختلاف في اتجاه إجابات أفراد العينة المبحوثة حول مدى اعتبارهم أن ضعف الثقافة الرقمية سبب رئيسي في انتشار الاحتيال الإلكتروني، وذلك حسب المتغيرات الشخصية (الجنس، السن، المستوى التعليمي، وعدد ساعات استخدام مواقع التواصل الاجتماعي يوميًا)، حيث وجدنا:

- بالنسبة للجنس:

أغلب الذين وافقوا تمامًا على أن ضعف الثقافة الرقمية سبب رئيسي في انتشار الاحتيال الإلكتروني هم الذكور بنسبة 11%، كما أن الذين وافقوا على ذلك من الذكور أيضًا بلغت نسبتهم 11%. في حين أن أغلب من وافقوا تمامًا من الإناث بلغت نسبتهم 25%، واللواتي وافقن فقط بنسبة 35%. وعموماً نجد أن كلا الجنسين يميلان للموافقة، لكن نسبة الموافقة التامة كانت أعلى لدى الإناث بنسبة 25% مقارنة بـ 11% لدى الذكور، مما يدل على وعي نسبي أكبر لدى النساء بخطورة ضعف الثقافة الرقمية.

- بالنسبة للسن:

نلاحظ أن أغلب الأفراد الذين تتراوح أعمارهم من 18 إلى 30 سنة وافقوا على الفرضية بنسبة 26%، ووافقوا تمامًا بنسبة 15%، أي أن المجموع بلغ 41%. أما الذين تتراوح أعمارهم من 31 إلى 50

سنة فقد بلغت نسبة الموافقة 19% ونسبة الموافقة التامة 16%، أي مجموع 35%. في حين نجد أن فئة 50 سنة فما فوق وافقوا بنسبة 1% ووافقوا تمامًا بنسبة 5% فقط، أي مجموع 6%. وعموماً نجد أن فئة الشباب بين 18 و30 سنة أكثر إدراكًا لعلاقة ضعف الثقافة الرقمية بانتشار الاحتيال الإلكتروني مقارنة بباقي الفئات.

- بالنسبة للمستوى التعليمي:

نجد أن أغلب الأفراد الذين لهم مستوى جامعي وافقوا على الفرضية بنسبة 22%، ووافقوا تمامًا بنسبة 22%، أي ما مجموعه 44%، وهي أعلى نسبة. أما الأفراد الذين لهم مستوى ثانوي فقد وافقوا بنسبة 17% ووافقوا تمامًا بنسبة 6% (مجموع 23%). في حين أن الأفراد ذوي المستوى المتوسط وافقوا بنسبة 6% ووافقوا تمامًا بنسبة 3% (مجموع 9%)، أما الأفراد ذوي المستوى الابتدائي فوافقوا بنسبة 1% ووافقوا تمامًا بنسبة 5% (مجموع 6%). وعموماً، نجد أن كلما ارتفع المستوى التعليمي زاد الوعي بكون ضعف الثقافة الرقمية سببًا في انتشار الاحتيال الإلكتروني.

- بالنسبة لعدد ساعات استخدام مواقع التواصل الاجتماعي يوميًا:

أغلب الأفراد الذين يستخدمون مواقع التواصل الاجتماعي من 4 إلى 6 ساعات يوميًا وافقوا على الفرضية بنسبة 17%، ووافقوا تمامًا بنسبة 12% (مجموع 29%). أما الذين يستخدمونها من 1 إلى 4 ساعات فقد وافقوا بنسبة 17%، ووافقوا تمامًا بنسبة 14% (مجموع 31%). بينما الذين يستخدمونها أقل من ساعة واحدة وافقوا بنسبة 2% ووافقوا تمامًا بنسبة 1% (مجموع 3%). وعمومًا نلاحظ أن الأفراد الذين يستخدمون وسائل التواصل الاجتماعي لفترات أطول هم أكثر وعيًا بخطورة ضعف الثقافة الرقمية ودورها في تسهيل عمليات الاحتيال الإلكتروني.

20. هل سبق أن تعرضت لعملية احتيال إلكتروني عبر مواقع التواصل الاجتماعي (السن، العمر، المستوى التعليمي، عدد ساعات استخدام مواقع التواصل الاجتماعي)

الجدول 24: توزيع افراد العينة حسب أن سبق لهم التعرض لعملية احتيال إلكتروني عبر مواقع التواصل الاجتماعي(السن، العمر، المستوى التعليمي، عدد ساعات استخدام مواقع التواصل الاجتماعي)

			هل يبق أن تعرضت لعملية احتيال إلكتروني عبر مواقع التواصل الاجتماعي؟					**المجموع**
			غير موافق تماما	**غير موافق**	**محايد**	**موافق**	**موافق تماما**	
الجنس	ذكر	التكرار	2	12	3	6	1	24
		النسبة%	2%	12%	3%	6%	1%	24%
	أنثى	التكرار	9	41	11	14	1	76
		النسبة%	9%	41%	11%	14%	1%	76%
	المجموع	التكرار	11	53	14	20	2	100
		النسبة%	11%	53%	14%	20%	2	%100
السن	من 18 إلى 30 سنة	التكرار	5	24	6	12	2	49
		النسبة%	5%	24%	6%	%12	2%	49%
	من 31 إلى 50 سنة	التكرار	5	26	6	7	0	44
		النسبة%	5%	26%	6%	7%	0%	44%
	50 سنة فما فوق	التكرار	1	3	2	1	0	7
		النسبة%	1%	3%	2%	1%	0%	7%
	المجموع	التكرار	11	53	14	20	2	100
		النسبة%	11%	53%	14%	20%	2%	%100
المستوى التعليمي	ابتدائي	التكرار	0	5	2	2	0	9
		النسبة%	%0	%5	%2	2%	%0	%9
	متوسط	التكرار	1	8	1	3	0	13

		النسبة%	%1	%8	1%	3%	%0	13%
	ثانوي	التكرار	4	18	3	4	0	29
		النسبة%	%4	%18	3%	4%	%0	%29
	جامعي	التكرار	6	22	8	11	2	49
		النسبة%	%6	%22	8%	11%	%2	%49
	المجموع	التكرار	11	53	14	20	2	100
		النسبة%	%11	%53	14%	20%	2%	%100
عدد ساعات استخدام مواقع التواصل الاجتماعي يوميا	أقل من ساعة واحدة من 1 إلى 4 ساعات	التكرار	0	4	1	0	0	5
		النسبة%	0%	4%	1%	0%	0%	5%
	من 4 إلى 6 ساعات	التكرار	2	13	1	9	0	25
		النسبة%	2%	13%	1%	9%	0%	25%
	أقل من ساعة واحدة من 1 إلى 4 ساعات	التكرار	1	26	5	5	1	38
		النسبة%	1%	26%	5%	5%	%1	38%
	من 4 إلى 6 ساعات	التكرار	8	10	7	6	1	32
		النسبة%	8%	10%	7%	6%	1%	32%
	المجموع	التكرار	11	53	14	20	2	100
		النسبة%	11%	53%	14%	20%	2%	%100

نلاحظ من خلال الجدول السابق وجود تباين واختلاف في اتجاه إجابات أفراد العينة المبحوثة حول مدى تعرضهم للاحتيال الإلكتروني عبر مواقع التواصل الاجتماعي، وذلك حسب المتغيرات الشخصية (الجنس، السن، المستوى التعليمي، وعدد ساعات استخدام مواقع التواصل الاجتماعي يوميًا)، حيث وجدنا:

- بالنسبة للجنس:

أغلب الذكور صرحوا بأنهم غير موافقين على أنهم تعرضوا للاحتيال بنسبة 12%، تليها نسبة 6% ممن وافقوا، ونسبة 3% كانت محايدة. بينما بلغت نسبة الموافقة التامة 1% فقط.

أما بالنسبة للإناث، فقد بلغت نسبة اللواتي غير موافقات 41%، و14% وافقن على أنهن تعرضن للاحتيال، في حين أن نسبة المحايدات كانت 11%، والموافقة التامة

لم تتعد 1.%

وعمومًا، نلاحظ أن كلا الجنسين يميلان إلى نفي التعرض للاحتيال الإلكتروني، ولكن نسبة الرفض كانت أعلى لدى الإناث (41%) مقارنة بالذكور (12%)، ما قد يدل على إما قلة تعرضهن فعليًا أو تحفظ أكبر في التصريح بذلك .في حين تبقى نسبة الموافقة على التعرض أعلى قليلاً لدى الإناث (15%) مقارنة بالذكور.(7%)

- بالنسبة للسن:

نلاحظ أن أغلب الأفراد الذين تتراوح أعمارهم من 18إلى 30 سنة صرحوا بعدم تعرضهم للاحتيال بنسبة 24%، ووافق 12% منهم على أنهم تعرضوا، و2% وافقوا تمامًا، أي أن نسبة الموافقة الكلية بلغت 14.% أما الأفراد الذين تتراوح أعمارهم من 31إلى 50 سنة فقد صرح 26% منهم بعدم تعرضهم، و7% وافقوا فقط على تعرضهم، دون تسجيل أي موافقة تامة، أي نسبة الموافقة الكلية 7.%أما فئة 50سنة فما فوق فقد سجلت أقل نسبة من الموافقة، إذ لم تتجاوز 1% فقط، بينما بلغت نسبة غير الموافقين 3.%

وعمومًا نجد أن فئة الشباب بين 18 و30 سنة أكثر تصريحًا أو وعيًا بوقوعهم في الاحتيال الإلكتروني مقارنة بباقي الفئات العمرية، مما يعكس ارتباطًا مباشرًا بين كثافة الاستخدام الرقمي والتعرض لمخاطر الفضاء الإلكتروني.

- بالنسبة للمستوى التعليمي:

تبين أن الأفراد ذوي المستوى الجامعي سجلوا أعلى نسب من الموافقة، حيث وافق 11% على أنهم تعرضوا للاحتيال و2% وافقوا تمامًا، أي ما مجموعه 13%، في حين بلغت نسبة غير الموافقين 22.% أما الأفراد ذوي المستوى الثانوي فقد وافق 4% فقط على تعرضهم دون تسجيل أي موافقة تامة، في حين أن 18% لم يوافقوا على ذلك. أما المستوى المتوسط فقد سجل 3% من الموافقة، في حين لم يسجل أي موافقة تامة. بينما الأفراد ذوي المستوى الابتدائي لم يوافقوا تمامًا إطلاقًا، وسجلوا فقط 2% كموافقة بسيطة.

وعموما نلاحظ أنه كلما ارتفع المستوى التعليمي، زادت نسبة التصريح بالتعرض للاحتيال الإلكتروني، مما قد يدل على أن أصحاب المستويات التعليمية العليا لديهم وعي أكبر بالمخاطر الرقمية وقدرة أفضل على تمييزها أو الاعتراف بها.

- بالنسبة لعدد ساعات استخدام مواقع التواصل الاجتماعي يوميًا:

نلاحظ أن الأفراد الذين يستخدمون مواقع التواصل من 1إلى 4 ساعات يوميًا سجلوا نسبة موافقة على التعرض للاختراق بلغت 5%، و1% موافقة تامة، أي مجموع 6%. أما الذين يستخدمونها من 4 إلى 6 ساعات فقد بلغت نسبة الموافقة 6% والموافقة التامة 1%، أي مجموع 7.% في المقابل لم يسجل الأفراد الذين يستخدمونها أقل من ساعة واحدة يوميًا أي نسبة موافقة أو موافقة تامة، مما يعكس ضعف احتمالية تعرضهم أو عدم وعيهم الكامل بحدوث الاحتيال.

وعموما نلاحظ أن الأفراد الذين يستخدمون وسائل التواصل الاجتماعي لفترات أطول هم أكثر تعرضًا أو وعيًا بإمكانية الاحتيال الرقمي، ما يبين وجود علاقة طردية بين مدة الاستخدام ومخاطر الوقوع ضحية للاحتيال.

رابعا: النتائج والاستنتاجات

1. أهم النتائج

تم التوصل إلى مجموعة من النتائج المهمة من خلال تحليل استبيان موزّع على عينة من مستخدمي مواقع التواصل الاجتماعي المهتمين بالبيع الإلكتروني، وقد تم تلخيص أبرز هذه النتائج فيما يلي:

على مستوى الخصائص الشخصية للعينة:

- يغلب على العينة الطابع الأنثوي بنسبة 76%، ما يشير إلى مشاركة نسوية قوية في البيئة الرقمية التجارية.
- تمثل الفئات العمرية بين 18 و50 سنة نسبة 93% من العينة، وهي الفئة الأكثر نشاطًا على الإنترنت.
- ما يقارب نصف العينة (49%) تحمل مستوى تعليمي جامعي، ما يوفّر بيئة مناسبة للوعي المعرفي بالمخاطر الرقمية.
- 70%من العينة يستخدمون مواقع التواصل لأكثر من 4 ساعات يوميًا، مما يرفع من احتمالية التعرض لمحاولات الاحتيال.

على مستوى الوعي والتجربة الشخصية مع الاحتيال الإلكتروني:

- 22%فقط أقروا بتعرضهم الشخصي للاحتيال، لكن 50% يعرفون ضحايا آخرين، ما يبرز وجود الظاهرة في المحيط.
- 42%يتلقون رسائل أو روابط مشبوهة بانتظام، مما يشير إلى نشاط فعلي لأساليب الاحتيال الرقمي.
- نسبة مرتفعة (75%) تشعر بالقلق من الوقوع ضحية للاحتيال، وهو ما يعكس إدراكًا متناميًا للمخاطر.

على مستوى المهارات والسلوكيات الوقائية:

- 60% يجدون صعوبة في التمييز بين الصفحات الأصلية والمزيفة، ما يعبّر عن ضعف في المهارات التفاعلية.
- 50% فقط يعرفون كيف يحمون حساباتهم.
- 35% لا يستخدمون خاصية التحقق بخطوتين، رغم أهميتها، و24% ينقرون أحيانًا على روابط مشبوهة.
- 56% يستخدمون كلمات مرور قوية، و54% يراجعون إعدادات الأمان دوريًا، ما يشير إلى بداية وعي أمني نسبي.

على مستوى المعرفة والتكوين في الثقافة الرقمية:

- 44% لا يتابعون محتوى الأمن الرقمي، و68% لم يشاركوا في أي ورشة أو دورة تدريبية.
- هذه المعطيات تبرز وجود فجوة معرفية وضعفًا في التكوين المنهجي، رغم تعرض المستخدمين لخطر دائم.

على مستوى العلاقة بين الثقافة الرقمية والاحتيال الإلكتروني:

- 84% من المشاركين يرون أن الثقافة الرقمية تقلل من فرص الاحتيال.
- 83% يؤمنون أن زيادة المعرفة الرقمية تساهم في الوقاية.
- 82% يرجعون سبب انتشار الاحتيال إلى ضعف الوعي الرقمي.
- 90% يدعمون إدراج الثقافة الرقمية في المناهج، و92% يرون أن التوعية المجتمعية ضرورة ملحة.

2. الاستنتاجات

انطلاقًا من النتائج السابقة، يمكن استخلاص الاستنتاجات التالية:

- وجود وعي نظري عالٍ مقابل ضعف في الممارسة الفعلية:

رغم أن غالبية المبحوثين يعترفون بأهمية الثقافة الرقمية، إلا أن سلوكياتهم الوقائية لا تعكس ذلك دائمًا. هذا التناقض بين المعرفة والممارسة يشكّل ثغرة مهمة يستغلها المحتالون.

- ضعف التكوين الرقمي:

معظم الأفراد لم يشاركوا في ورش أو برامج تدريبية، وهو ما يجعل معرفتهم محدودة بالمهارات التقنية الأساسية، رغم أن الكثير منهم يستخدمون مواقع التواصل لأغراض تجارية.

- العينة ميدانيًا مستهدفة بشكل واضح:

بما أن الاستبيان نُشر في صفحة بيع إلكتروني، فإن المشاركين منخرطون في بيئة رقمية مشبعة بالإعلانات والروابط، ويظهر أن الكثير منهم يتلقون بالفعل رسائل وروابط مشبوهة، ما يجعلهم في دائرة الخطر اليومي.

- الثقافة الرقمية شرط أساسي للوقاية:

هناك إدراك جماعي بأن الثقافة الرقمية ليست مجرد خيار، بل ضرورة للحماية الشخصية. وارتبط هذا الوعي بالمطالبة بإدراجها في المناهج التعليمية وتكثيف التوعية المجتمعية.

الخاتمـــــــــــة

خاتمـــــــــة

وفي ختام دراستنا هاته نخلص أن لثقافة الرقمية تأثير كبير على المستخدمين لمواقع التواصل الاجتماعي لتزويدهم بالمعلومات الرقمية، في مختلف المجالات خاصة في مجال الحماية للمستخدم في وسط البيئة الرقمية وذلك لعدم تعرضه للجرائم الالكترونية التي أصبحت ظاهرة منتشرة بكثرة .

ومن ابرز هاته الجرائم الإلكترونية لدينا الاحتيال الالكتروني الذي بات منتشرا بصورة رهيبة وسط المستخدمين الذين يفتقرون لثقافة الرقمية ، ولديهم فجوة رقمية مما يساعد المحتالين على استغلال هاته الفجوات والثغرات لتفنن في طرق الاحتيال فلذلك برزت مجموعة من الاستراتيجيات التي تساهم في نشر الثقافة الرقمية، وخلق لديهم ما يعرف بالتربية الرقمية التي هي استخدام التكنولوجيا التي تسمح لكل فرد بالمشاركة الفعالة في مختلف مجالات الحياة سياسيا أو اجتماعيا أو غير ذالك ويشترط أن يكون الاستخدام المشار إليه أخلاقيا وآمنا، وقد زاد الطلب على التربية الرقمية بعد انتشار السلوكيات غير اللائقة ، كما أن نشر الثقافة الرقمية قد يساعد المستخدمين لتطوير مهاراتهم الرقمية وذلك من خلال إمكانهم للكشف عن أساليب الاحتيال لعدم الوقوع ضحية له.

إلى أن نسبة الثقافة الرقمية في وسط مجتمعنا لا تزال قليلة نوعا ما وذلك لعدم توفر الإمكانيات الأزمة وليس لها جانب خاص مهتم بها فلهذا السبب يجب توفير مساحة خاصة لثقافة الرقمية وإدراجها ضمن المناهج المدرسية وتدريسها في شتى المؤسسات لأنها فعلا أصبحت من الضروريات في الوقت الحالي لأنه وقت السرعة والتطور والتكنولوجيا فلذلك لابد من بناء مجتمع مثقف رقميا لتفادي أضرار هذا الوسط الرقمي الخطير لأنه على الرغم من ايجابيات هذا التطور إلى ان هناك العديد من السلبيات.

التوصيات والاقتراحات

1. **تعزيز الثقافة الرقمية لدى المستخدمين:**

- إطلاق حملات توعية مستمرة حول مخاطر الاحتيال الإلكتروني.
- إدراج الثقافة الرقمية كمادة تعليمية في المدارس والجامعات.

2. **رفع الوعي الأمني الرقمي:**

- نشر دليل توعوي رقمي خاص بمستخدمي "بريدي موب" يوضح كيفية الحماية من الاحتيال.
- تنظيم دورات تدريبية افتراضية وميدانية حول السلامة الرقمية.

3. **التعاون بين الجهات الحكومية والقطاع الخاص:**

- التنسيق بين بريد الجزائر ووزارة التعليم لنشر ثقافة الحذر الرقمي وتوسيع نطاق التربية الرقمية.
- تشجيع منصات التواصل على حذف الحسابات الاحتيالية بشكل أسرع.

الاقتراحات

1. **توسيع نطاق الدراسة:**

- مقارنة بين مستويات الوعي الرقمي في ولايات جزائرية مختلفة.
- دراسة العلاقة بين الفئة العمرية أو المستوى التعليمي وخطر التعرض للاحتيال.

2. **تحليل فني لثغرات التطبيقات المالية:**

- دراسة تقنية لمستوى الأمان في تطبيقات الدفع الإلكترونية.

3. **تقييم فعالية الحملات التوعوية:**

- إجراء دراسات لاحقة لقياس تأثير حملات التحسيس في الحد من الاحتيال

قائمة المراجع

مصادر و مراجع الدراسة

المراجع باللغة العربية :

أولا : الكتـــــب

1. إيهاب خليفة، مواقع التواصل الاجتماعي أدوات التغيير العصرية عبر الإنترنت، المجموعة العربية للتدريب والنشر، الطبعة الأولى ،2016.
2. حكيم يونس كرو العزاوي: مقدمة في منهج البحث العلمي، دار دجلة ناشرون وموزعون، الطبعة الأولى، عمان الأردن،2008، ص180.
3. رضوان مفلح العالي، وآخرون، مدخل إلي وسائل الإعلام الإليكتروني والفضائي، دار المكتبة الحامد، عمان، الأردن، ط1، 2016 ص206.
4. سنوسي حياة، الثقافة الرقمية، قراءة تحليلية فى المفهوم وعوامل اكتسابها، جامعة يحي فارس المدية، 10 أكتوبر 2022, ص 309.
5. سعد سلمان المشهداني، منهجية البحث العلمي، دار أسامة، ط1, عمان، الأردن، 2019، ص 85.
6. عادل محمد عادل، مناهج البحث العلمي في العلوم الانسانية, ط1 دار الشروق لنشر والتوزيع، عمان 2014, ص60.
7. عبد الرحمان بن إبراهيم الشاعر، مواقع التواصل الاجتماعي والسلوك الإنساني، ط1، عمان، دار الصفاء للطابعة والنشر والتوزيع، 2015، ص63-64.
8. علي سيد إسماعيل، مواقع التواصل الاجتماعي بين التصرفات المرفوضة والأخلاقيات المفروضة، بحث مقدم لجائزة خدمة الدعوة والفقه الإسلامي، دار التعليم الجامعي للنشر والتوزيع، 2020، ط الإسكندرية، 2019، ص20.
9. فيصل محمد عبد الغفار
10. ماهر عودة الشمالية، وآخرون، الإعلام الرقمي الجديد، دار الإعصار العالمى، ط1، 2015، ص 201 .

11. محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير مشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة 2009, ص 32.
12. محمد سامي راضي منهج البحث العلمي في المجال الإداري ،دار التعليم الجامعي للطباعة والنشر والتوزيع ، الاسكندرية ،2012ص118.

ثانيا : الأطروحات و الرسائل

13. أحمد قاسمي، سليم جداي، تأثير مواقع التواصل الاجتماعي على الأمن المجتمعي لدول الخليجية، المركز الديمقراطي، العربي لدراسات الإستراتيجية الاقتصادية والسياسية، برلين ألمانيا، ط 1، 2019, ص18.
14. خليل شدان يعقوب اثر مواقع التواصل الاجتماعي على الوعي السياسي بالقضية الفلسطينية لدى طلبة النجاح الوطنية، رسالة مجستير في التخطيط التنمية السياسية، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2015، ص30.
15. محمد هشام صالح عبد الفتاح، جريمة الإحتيال دراسة مقارنة، اطروحة لاستكمال درجة الماجيستير في القانون العام ،كلية الدراسات الوطنية، نابلس، فلسطين، 2008، ص 8و9.

ثالثا : محاضرات جامعية

16. الدكتورة عبيديش، ملخص مقياس مناهج وتقنيات البحث في علوم الإعلام والاتصال، سنة ثانية ، جامعة الجزائر، 3 كلية علوم الاعلام والاتصال قسم علوم الاعلام.
17. هواري سعاد، أساليب الاستبيان (ثانية ماستر) دروس الثلاثي الثالث، اختصاص الدول الديناميكية المجالية والتسيير، قسم التهيئة العمرانية، كلية علم الأرض والجغرافيا والتهيئة العمرانية، جامعة الإخوة منتوري، جامعة قسنطينة 1، الجزائر، ص3 .

رابعا : البحوث و الندوات

18. بوخبزة نبيلة، بن تومي فضلة، شبكات التواصل الاجتماعي : نحو تشكيل فضاء مستحدث للهوية الإفتراضية المجالات الاجتماعية التقليدية والحديثة وإنتاج الهية الفردية في المجتمع الجزائري، الملتقى الدولي الثاني، جامعة قاصدي، ورقلة، 2014، ص540.

19. تلفزيون سوريا ،اسطنبول ،كيف تحمي نفسك من عمليات الإحتيال الالكتروني؟ إليك 6 نصائح ذهبية.
20. جمعية الإجتماعيين العمانية إلى وزارة التنمية الإجتماعية، سلطنة عمان ،2020، ص50.
21. جهان حداد، المقاهي الإلكترونية ودورها في التحول الثقافي فى مدينة إربد، دراسة أنثربولوجية ،جامعة اليرموك،رسالة ماجستير ، غير منشورة ،2002م ص، 28
22. رشيد حسين 6 نوفمبر 2020 الثقافة الرقمية مفهوم وفهم، تاريخ الاسترداد،06 نوفمبر 2020، من دنيا الوطن .
23. سلطان بن محمد الهاشمي وآخرون، أثر إستخدام وسائل التواصل الإجتماعي على تنشئة الطفل في المجتمع العماني التعليمية الإجتماعية النفسية الصحية.
24. السماك عبد فتحي غانم إسراء(11-12شباط 2019) ، توظيف الثقافة الرقمية ف إدارة الوقت عند مديري المدارس الثانوية من وجهة نظر المشرفين التربويين ،المؤتمر العلمي الدولي الأول العلوم الإنسانية والصرفة رؤية نحو التعليم والتربية المعاصرة نقابة الأكاديميين العراقيين ،جامعة دهوك ،العراق ، ص639.
25. الملتقى الثاني للثقافة الرقمية، تطوير المهارات في العصر الرقمي – الابتكار التواصل – والخصوصية ، المنظمة العربية لتنمية الإدارية ،12 فبراير 2025.
26. محمد عبدو، الإحتيال في التجارة الإلكترونية الأنواع الشائعة وطرق الحماية والمواجهة 26، افريل 2021 expandcart.
27. المدونة العربية لتنمية الإدارية الملتقى العربي الأول لتحول الرقمي "دور واهمية الثقافة الرقمية في تعزيز سياسات التحول الرقمي ": الفرص والتحديات 03-مارس إلى 05 ماي 2024.
28. نعيم فيصل المصري، إستخدامات الطلبة الجامعيين لمواقع التواصل الإجتماعي وأثرها على وسائل الإعلام الأخرى، دراسة مقدمة لمؤتمر الإعلام والتحولات المجتمعية، كلية الإعلام بجامعة اليرموك، الأردن ،2011، ص43.
29. هيئة الحكومة الرقمية .دراسة بحثية الإحتيال الرقمي، اصدار 1 ، أغسطس 2023.
30. هيلي كوميبتون، كيف يستخدم المحتالون فيسبوك ماركت للنصب على ضحاياهم ، تحقيقات بيبيسي، 02ابريل 2024.

خامسا : المقالات العلمية و المجلات

31. إليسون نيكول، بويد دانا ، مواقع التواصل الإجتماعي التعريف والتاريخ والدراسات، مجلة الاتصالات عبر الحاسوب ،المجلد 13 ، العدد 1، أكتوبر 2007، ص 2010-230.

32. بلال عقل الصنديد مقال الاحتيال الالكتروني وتحدياته المستمرة.

33. بن زينب فاطمة 2019 فضاءات المطالعة العمومية ودورها في تفعيل ونشر ثقافة المعلومات والثقافة الرقمية، المجلة العربية للارشيف والتوثيق والمعلومات، س23 العدد 46، ص420-421.

34. بولحية شهيرة ، سويح دنيا زاد ، الاحتيال الالكتروني ، مقال مجلة الدراسات القانونية والاقتصادية المركز الجامعي سي الحواس بريكة.

35. بيان عبد اللطيف، مفهوم الإحتيال الإلكتروني وكيفية تجنب الوقوع فيه، مقال ،الشارقة 24، 16 ديسمبر 2024، 02:58 AM.

36. حرز الله محمد لخضر، الجرائم الرقمية والأمن الفكري، جناية الافتراضي على الواقعي ، مدونات الجزيرة aljazeera.net، 09/02/2020

37. حسين شفيق مواقع التواصل الاجتماعي :ادوات ومصادر للتغطية الاعلامية دار الفكر وفن الطباعة والنشر والتوزيع.

38. خالد بن ثاني آل ثاني، رئيس التحرير : جابر سالم الحربي ، تعرف على أساليب الاحتيال الإلكتروني وطرق الحماية ، مجلة الشرق ، 11جانفي 2019 بتوقيت 01:58

39. خليل سمير (1971) ، دليل مصطلحات الدراسات الثقافية والنقد الثقافي ، إظافة توثيقية للمفاهيم الثقافية المتداولة ، بيروت ، دار المكتب العلمية ص 12.

40. دليو ،فضيل، **اختيار العينة في البحوث الكيفية** ، مجلة البحوث ودراسات في الميديا الجديدة ، المجلد ،03 العدد 03 ، جامعة محمد بوضياف المسيلة ،ص 12.

41. رحاب مصطفى كامل ،دور الثقافة الرقمية في تحقيق الاستدامة الاجتماعية وسد الفجوة الرقمية ، دراسة تحليلية للمفاهيم في ظل تداعيات كوفيد 19، المجلة الدولية للسياسات العامة في مصر . ijppe.journals.ekb.eg

42. رمضان محمود عبد العليم عبد القادر ، 2019 الثقافة الرقمية لدى طلاب الدراسات العليا التربوية بالجامعات المصرية في ضوء متطلبات الاقتصاد القائم على المعرفة ، مجلة كلية التربية ،العدد 184، الجزء الثالث ، جامعة الأزهر ، مصر ، ص 1548.
43. رواية احمد القحطاان وسعود بن الضحيان ، **النمطية المنهجية في الرسائل الجامعية** ، دراسة مطبقة علي عينة من رسائل الدكتوراه بجامعتي الملك سعود والإمام محمد بن سعود الإسلامية .
44. زاهر راضي، إستخدام مواقع التواصل الإجتماعي في العالم العربي، مجلة التربية ،ع15 ،جامعة عمان الأهلية ،عمان 2003، ص23.
45. الزهرة الأسود العينات في البحث العلمي إجراءات واعتبارات، مجلة تنوير للبحوث الإنسانية والاجتماعية ، دم 12, جامعة الوادي الجزائر، ص 264-265.
46. سليم احمد غرت (2008)، الثقافة الرقمية في اطار التغيرات الاجتماعية والقيم الانسانية ، مجلة دنيا الوطن، 15اكتوبر.
47. شارف عبد القادر ورمضاني لعلا ، التحديات العربية لتضييق الفجوة الرقمية ،مجلة النصر الاقتصادية ، العدد 6، جامعة بشار ، الجزائر ،ص 218.
48. طارق محمد محمد السعيدي ، الثقافة الرقمية عبر وسائل التواصل الاجتماعي وعلاقتها بتنمية المواطنة الرقمية ، مجلة إتحاد الجامعات العربية لبحوث الاعلام وتكنولوجيا الاتصال ، المجلد 2022, العدد 9، الرقم المسلسل للعدد 9 الجزء الثاني ، ص310.
49. عبيد على، ناصر موفق وآخرون ، ماهية جريمة الإحتيال الإلكتروني ، مجلة كلية القانون للعلوم القانونية والسياسية ، كلية الحقوق جامعة تكريت ،بغداد ص 336.
50. فوزية محمدي ، تأثير العنف الإلكتروني في مواقع التواصل الإجتماعي على العلاقات الإجتماعية لدى الشباب، دراسة ميدانية بمدينة ورقلة ،جامعة ورقلة، مقال نشر في مجلة جيل العاوم الإنسانية والإجتماعية ، العدد 40، ص47.
51. لولي حسيبة ، الثقافة الرقمية، في وسط الشباب، مجلة العلوم الإنسانية والإجتماعية، عدد 29، 2017، ص 67.
52. مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية العدد العشرون، جامعة القيوم ، مصر ،2020، ص 446.

53. مجلة الأخبار ،استراتيجية ورش عمل لثقافة الرقمية ، 2024/08/30.
54. وائل مبارك خضر فضل الله ،أثر فايسبوك على المجتمع ، شمس النهضة الخرطوم ، السودان ،2010 ، ص7.
55. نبيل علي ونادية حجازي ، الفجوة الرقمية ، سلسلة عالم المعرفة ، الكويت 2005 ، ص26.

سادسا : المواقع

56. موقع الباحثين،https://arab-scholars.com / ، تم الاطلاع يوم: 09جانفي 2025
57. هشام مدخنة،100 دولار خسائر الشركات من الإحتيال الودي سنويا، https://www.alkhaleej.ae/، 27 يوليو 2024 .
58. موقع Tookitaki، الاحتيال الالكتروني أمثلة واقعية وإستراتيجيات الوقاية، https://explore.tookitaki.com/، ديسمبر 2024.
59. موقع قوقل مايكروسفت، https://www.microsoft.com/ar/microsoft-teams/log-in?market=، تم الاطلاع يوم :12 جانفي 2025.
60. وليد ناصر ، إحتيال التسويق ،.موقع عرفني،https://www.3arrafni.com/ ، تم الاطلاع يوم :11 جانفي 2025.
61. موقع إلكتروني https://sharjah24.ae،اسباب وانواع الجرائم الالكترونية وسبل مكافحتها ، يوم الاستطلاع 12 جانفي 2025.
62. سايبر وان ، ما هو الإحتيال الإلكتروني ، الأمن السيبراني،https://cyberone.com /، يوم الاستطلاع 10 جانفي 2025.
63. موقع الكتروني ، البرمجيات الخبيثة للاحتيال الإلكتروني https://www.aljazeera.net
64. إلهام هواري ،تحذير عاجل لمستخدمي بريدي موب من الإحتيال الإلكتروني ، awras.com بتاريخ 2025/04/06
65. البنك السعودي للإستثمار، كيف تحمى نفسك من الإحتيال عبر وسائل التواصل الإجتماعي ، Linkedin 2025/جانفي/14
66. Star7arabطريقة جديدة للنصب والإحتيال عبر تطبيق بريدي موب 2020/02/12

67. مستخدم ، الفجوة الرقمية ، موقع جامعة محمد خيضر بسكرة ,– elearning.univ-biskra.dz ، 23 ماي 2025 9:46

68. عمر عبد الجبار ، **مجتمع الدراسة وانواع العينات**، اجتماعي موقع الدكتور مولود زايد الطبيب , ejtema3e.com، 23 جانفي 2025 15:36

سابعا: المقابلات

69. حمد العمري، مصلحة النقدية، تعريف تطبيق بريدي موب، مديرية بريد الجزائر ورقلة ، (20مارس2023مقابلة شخصية)

70. دليل الاحتيال عبر مواقع التواصل الاجتماعي ، ماهي عمليات الاحتيال على وسائل التواصل الاجتماعي ؟, مركز استشارات ادارة الأموال عبر الانترنت ،internetmatters.org

ثامنا : وثائق

71. وثائق المؤسسة

72. حملة تحسيسية من أجل استخدام آمن للبطاقة الذهبية وتطبيق بريدي موب

المراجع باللغة الاجنبية :

73. Fnancial fraud exploring types and beyond. www-fraud-com-translate.goog

74. Sean Michael kerner Dijital culture october 2023 www-techtarget-com.translate.goog

75. A.coleman.PH.D What is a Digetal Coultoure and why is it important ? . march 21 2024 , delecarnegie.com.

76. Shanxing Du,Does digital literacy help residents avoid becomiing victims of frauds? Empirical evidence baseden survey of residents in six provinces of east china .international Review of Economics &finance, March 2024 ,Pages,364-377

77. Door Alexander van Deursen en Jan van Dijk , The Dijital divide, An introduction University of Twente, utwente.nlut

الملاحـــــــق

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد خيضر _ بسكرة

كلية العلوم الإنسانية والإجتماعية

قسم علوم الإعلام والإتصال

تخصص: إعلام سمعي بصري

مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والإتصال – تخصص إعلام سمعي بصري

إستمارة إستبيان بعنوان:

الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي وعلاقته بالثقافة الرقمية
(دراسة مسحية لعينة من مستخدمي بريدي موب)

إعداد الطالبة: تحت إشراف الأستاذة

صبربن نخال ثوراي صونية

في إطار القيام بدراسة ميدانية ضمن متطلبات إنجاز مذكرة ماستر في علوم الإعلام والإتصال تخصص إعلام سمعي بصري، والمعنونة بـ " الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي وعلاقته بالثقافة الرقمية (دراسة مسحية لعينة من مستخدمي بريدي موب)

"، نضع هذا الإستبيان بين أيديكم ونستسمحكم عذرا في تخصيص جزءا من وقتكم في الإجابة على أسئلته.

فنرجوا منكم الإجابة بكل جدية وموضوعية لتزويدنا بالمعلومات المناسبة لهذا الموضوع، كما نحيطكم علما أن هذه المعلومات ستبقى سرية ولا تستخدم إلا لغرض البحث العلمي.

البيانات الشخصية

1. الجنس:

أنثى ☐

ذكر ☐

2. العمر:

من 18 سنة إلى 30 سنة ☐

من 30سنة إلى 50 سنة ☐

من 50 سنة فما فوق ☐

3. المستوى التعليمي

إبتدائي ☐

متوسط ☐

ثانوي ☐

جامعي ☐

4. عدد ساعات استخدام مواقع التواصل الإجتماعي يوميا.

أقل من ساعة ☐

من 1 إلى 3 ساعات ☐

من 4 إلى 6 ساعات ☐

أكثر من 6 ساعات ☐

المحور الغول : أسباب انتشار الاحتيال الالكتروني عبر مواقع التواصل الاجتماعي

5. هل سبق أن تعرضت لعملية إحتيال إلكتروني عبر مواقع التواصل الإجتماعي؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

6. هل تعرف شخصا تعرض للإحتيال الإلكتروني عبر مواقع التواصل الإجتماعي؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

7. هل تصلك رسائل أو روابط مشبوهة بشكل متكرر ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

8. هل تشعر بالقلق من الوقوع ضحية للإحتيال الإلكتروني ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

9. هل تجد صعوبة في التمييز بين الصفحات الحقيقية والمزيفة .

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

10. هل تعرف كيف تحمي حساباتك علي مواقع التواصل الإجتماعي؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

المحور الثاني : خطوات الحماية من الاحتيال الالكتروني وأهمية الثقافة الرقمية

11. هل تفعل خاصية التحقق بخطوتين لحساباتك الشخصية ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق أبدا ☐

12. هل تنقر على روابط من مصادر غير موثوقة ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

13. هل تستطيع التحقق من الصفحات الرسمية بسهولة ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

14. هل تتابع محتوى متعلقا بالأمن الرقمي ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

15. هل سبق أن شاركت في دورة أو ورشة حول الثقافة الرقمية أو الأمن الرقمي ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

16. هل تستخدم كلمات مرور قوية لكل حساب ؟

- أوافق بشدة ☐
- أوافق ☐
- محايد ☐
- لا أوافق ☐
- لا أوافق أبدا ☐

17. هل تراجع إعدادات الأمان في حساباتك بشكل دوري ؟

- أوافق بشدة ☐
- أوافق ☐
- محايد ☐
- لا أوافق ☐
- لا أوافق أبدا ☐

المحور الثالث : أهمية الثقافة الرقمية لتفادي الاحتيال الالكتروني لدي المتعاملين مع تطبيق بريدي موب

18. هل الثقافة الرقمية تقلل من نسبة تعرضك للإحتيال الإلكتروني ؟

- أوافق بشدة ☐
- أوافق ☐
- محايد ☐
- لا أوافق ☐
- لا أوافق أبدا ☐

19. هل الثقافة الرقمية تقلل من نسبة تعرضك للإحتيال الإلكتروني .

- أوافق بشدة ☐
- أوافق ☐
- محايد ☐
- لا أوافق ☐
- لا أوافق أبدا ☐

20. هل كلما زادت معرفتك رقمية قللت من فرص تعرضك للإحتيال الإلكتروني ؟

- أوافق بشدة ☐
- أوافق ☐
- محايد ☐
- لا أوافق ☐
- لا أوافق أبدا ☐

21. هل ضعف الثقافة الرقمة سبب رئيسي في انتشار الإحتيال الإلكتروني ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

22. هل من الضروري إدراج الثقافة الرقمية ضمن المناهج الدراسية ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐

23. هل التوعية المجتمعية ضرورية لمواجهة جريمة الإحتيال الإلكتروني ؟

أوافق بشدة ☐

أوافق ☐

محايد ☐

لا أوافق ☐

لا أوافق أبدا ☐


بريدي موب