التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي بسبب انتهاك الخصوصية والهجمات السيبرانية في المملكة العربية السعودية

(دراسة ميدانية)

أ/ فريد صالح كلنتن
د/ دعاء محمد سلمان

١. ملخص الدراسة:

من مميزات وسائل التواصل الاجتماعي التفوق التكنولوجي في مختلف النواحي الإيجابية والسلبية، وخلصت الدراسة بتجميع أراء المختصين في مجال التقنية الرقمية وعددهم (٣٠) عينة من القطاعات الحيوية اللائي لديهن مفهوم الأمن والإرهاب السيبراني بشكل أفضل، وعددًا من الأفراد العاديين يقدرون (٣٩) عينة اللائي لديهن تجارب فعلية وتأثروا بانتهاكات خصوصيتهن ، فكان عدد العينات (٦٩) عينة وتم جمع أراءهن بواسطة الاستبانة الإلكترونية، وتعد من الدراسات الوصفية الميدانية، وعلى ضوء توضيح الباحث فإن التطور في تكنولوجيا المعلومات يسير باتجاهين متعاكسين فبقدر تكثيف الحماية بالأمن السيبراني، بالمقابل يزيد من الاختراقات لوصول التكنولوجيا المعاكسة للخلايا الإرهابية، وأن الانتهاكات والإرهاب السيبراني يؤديان إلى فقدان الثقة في الأنظمة الرقمية، فتم صياغة المشكلة الرئيسية بمضمون

ماهي التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي في محاور (انتهاك الخصوصية، والهجمات السيبرانية، وفقدان الثقة في الأنظمة الرقمية)، وكان من بين الأسئلة الفرعية، ما تصور الشركات والمؤسسات في تعزيز استراتيجيات أمن المعلومات للحد من التهديدات السيبرانية، وكيفية قياس فعالية التدابير الأمنية المتخذة في مواجهة التهديدات السيبرانية في البيئة الرقمية، ومن بين الأهداف التوعية بأمن المعلومات وسبل تعزيز الوعي الرقمي لدى الجمهور والعاملين في هذا المجال، وتقييم السياسات والتشريعات الحالية المتعلقة بحماية الخصوصية وتقديم مقترحات لتعزيزها وتحسينها، والتوصل إلى مجموعة من التوصيات في ضوء ما سيتم التوصل إليه من النتائج التي سوف يتم الحصول عليها بحيث يمكن تطبيقها والاستفادة منها، وقد وضعت فرضيتين بهذا الخصوص، وكشفت نتائج الدراسة أن سياسة الخصوصية متشابهة في غالبية مواقع التواصل الاجتماعي، بالإضافة إلى استغلال المعلومات التي تجمعها عن المستخدمين لأن السياسة غير واضحة او غير مفهومة بالنسبة لجميع المستخدمين، وأن تلك الخدمات المجانية ليست في الواقع حقيقة، فهي تستفيد من المعلومات بطريقة أو بأخرى والتجارة بها، ويؤدي انتهاك الخصوصية بالقلق والضغط النفسي ، وتتسبب منصات الإعلام الاجتماعي والتفاعلية في صعوبة التمييز بين المعلومات الصحيحة والمضللة، وأن الإعلانات المستهدفة تزيد من قلق المستخدمين بشأن خصوصيتهم، فنرى أهمية التعليم والتثقيف الرقمي، فكانت التوصيات التوعية المجتمعية بمخاطر انتهاك الخصوصية في ظل سياسة إعلامية لتنبيه الجمهور وتوعيته بحقوقه، والضغط على إدارات مواقع التواصل الاجتماعي، لإجبارها على احترام الحق في الخصوصية، وإدراج منهج تعليمي حول التربية الإعلامية.

الكلمات المفتاحية: فقدان الثقة – الإعلام الرقمي – انتهاك الخصوصية – الهجمات السيبرانية

Challenges and risks of losing the trust in media in the light of digital media due to privacy violations and cyber-attacks in the Kingdom of Saudi Arabia

(A field study)

2. Abstract:

Social media has privileges in technological superiority in various positive and negative aspects. This study is concluded by aggregating experts' opinions in the field of digital technology, totaling 30 samples from vital sectors who have a better understanding of security and cyberterrorism. Additionally, the study comprises 39 samples of ordinary individuals, who have actual experiences and have been affected by privacy violations, resulting in a total sample size of 69. Their opinions were collected through an electronic questionnaire, constituting a descriptive field study. The researcher pointed out that the advancement in information technology is moving in two opposing directions: while enhancing cybersecurity protection, it simultaneously increases penetrations to provide technology to terrorist cells. Violations and cyberterrorism lead to losing the trust in digital systems. Thus, the main problem was formulated regarding the challenges and risks of losing trust in media in the era of digital media, focusing on privacy violations, cyber-attacks, and loss of trust in digital systems. Subsidiary questions included: how do companies and institutions envision enhancing information security strategies to mitigate cyber threats and how to measure the effectiveness of security measures taken to counter cyber threats in the digital environment? Among the objectives were exploring the importance of information security awareness and enhancing digital awareness among the public and professionals in this field, evaluating current policies and legislations related to privacy protection, providing suggestions to enhance and improve them, and reaching a set of recommendations in light of the results obtained for implementation and utilization. Two hypotheses were developed in this regard, and the study's results revealed that privacy policies are similar on most social media platforms, in addition to the exploitation of user-collected information because

the policy is unclear or incomprehensible to all users. Free services are not actually free; they benefit from information in one way or another and trade in it. Privacy violations cause anxiety and psychological pressures, leading to the deterioration of social relationships between users and digital media. Interactive media platforms make it difficult to distinguish between accurate and misleading information Targeted advertising increases users' concerns about their privacy, Hence, the importance of digital education and awareness in increasing awareness of the risks and challenges facing media trust in digital media. Therefore, the recommendations included societal awareness of the risks of privacy violations under a media policy to alert and educate the public about their rights, pressures on social media administrations to force them to respect privacy rights, and the inclusion of an educational curriculum on digital media.

Keywords: Losing trust - Digital Media - Privacy Violations - Cyber Attacks

٣. المقدمة

يمضي التقدم التكنولوجي قدمًا ، وقد أحدث تحولًا كبيرًا في تقارب البشر بعمليات التواصل في تكنولوجيا الإعلام الرقمي، وفي مجال المعلومات عبر وسائل التواصل الاجتماعي التي تزايدت تحدياتها ومخاطرها بإهمال القيم وكشف أسرار الأفراد والبيانات الشخصية، ففي شبكات التواصل التي أصبحت منظومة إعلامية متكاملة حيث ينشر المستخدمون بالصوت والصورة الحية والكتابات التفاعلية ما يريدون من تفاصيل حياتهم الشخصية والاجتماعية والعملية وحيث أنها السمة المميزة في العصر الرقمي إلا أنها تثير المخاوف في استغلال تلك البيانات والمعلومات والصور في عمليات الابتزاز الرقمي،(محمد،٢٠٢٢م). وأصبح انتهاك الخصوصية والهجمات السيبرانية يشكل تهديدًا كبيرًا على الأفراد والمؤسسات وتزايدت حالات انتهاك الخصوصية وسرقة البيانات، والتلاعب بالمعايير الأخلاقية والمهنية (الغيطي،٢٠٢١م)، مما يتطلب حماية الخصوصية والبيانات في عصر الإعلام الرقمي.

وتتعرض المؤسسات والهيئات لهجمات سيبرانية من قبل تنظيمات إرهابية تهدف إلى استغلال الثغرات في الأنظمة الرقمية والاستيلاء على المعلومات الحساسة، وتصاعدت حالات الاختراق السيبراني مما يبرز أهمية تعزيز الأمن السيبراني وتطوير برامجه لحماية البيانات والأنظمة الرقمية، وإن الهجمات السيبرانية لا تقتصر على صناعات محددة، فهي تستهدف القطاعات الحيوية في الاقتصاد العالمي مما يؤدي إلى اضطراب واسع النطاق، وأثبتت الإحصائيات أن المملكة العربية السعودية " هدفاً لهجمات سيبرانية إلكترونية فقد احتلت المركز ١٣ عالمياً والأولى عربياً في الأمن السيبراني ، وأشهر هجمة فيروسية "شمعون" عام ٢٠١٢م، الذي تسبب في شلل أجهزة الكمبيوتر بحوالي ٣٥,٠٠٠ جهاز كمبيوتر وأثر في الوزارات الحكومية وشركات البتروكيماويات. وهدف الهجوم إلى وقف إنتاج النفط والغاز في أكبر دولة

مصدرة في منظمة أوبك، **وابتُزَّت ٥٠ مليون دولار**." (المقرن،١٤٤٥). وارتفعت الهجمات السيبرانية خلال العام ٢٠٢٢ م بنسبة ٣٨% مقارنة بالعام الذي سبقه بناءً على التقارير، ويتوقع أن يشهد العام ٢٠٢٣ م نشاطًا أكبر في الهجمات الإلكترونية بحسب بيانات" تشيك بوينت."(تشيك بوينت،٢٠٢٣م).

إن دراسة وفهم هذه التحديات والمخاطر المرتبطة بالتقدم التكنولوجي في ظل الإعلام الرقمي من الأمور الأساسية لضمان استخدام آمن ومسؤول للتكنولوجيا والمعلومات من الوصول غير المصرح والاستخدام الخاطئ، ويزيد من التحديات الهجمات السيبرانية المتزايدة سواءً كانت اختراقات للأنظمة أو هجمات استنتاجية تهدف إلى سرقة البيانات أو تعطيل الخدمات الرقمية، فالتطور السريع في التكنولوجيا يجعلنا بحاجة مستمرة لتحديث وتطوير أنظمة وبرامج لمواكبة التقنيات الجديدة. ويتطلب ذلك استثمارات كبيرة في التكنولوجيا والتقنيات الحديثة في عالمنا اليوم.

٤. * الإطار النظري *

٥- مراجعة الأدبيات:

قسمت الدراسة إلى ثلاثة محاور، حيث تناول الباحث في المحور الأول انتهاك الخصوصية، والمحور الثاني الإرهاب السيبراني، والمحور الثالث فقدان الثقة في الأنظمة الرقمية.

١.٥ محور انتهاك الخصوصية :

- استهدفت دراسة (Fang،٢٠٢٣)، بعنوان " Social Media Changed the Notion of Privacy"، إلى تأثير وسائل التواصل الاجتماعي على المفاهيم التقليدية والمعاصرة، ويناقش كيف تطور الويب من ١.٠ إلى ٣.٠ على اتجاهات الخصوصية مع وجود التطبيقات الحديثة. ومع ظهور الويب ٣.٠، من المتوقع أن يتحكم المستخدمون في ملكية البيانات الرقمية ومعلوماتهم الشخصية. وأيضاً فإنها

تثير مخاوف بشأن انتهاكات الخصوصية، وتستكشف هذه الدراسة النتائج الإيجابية والسلبية لمشهد الخصوصية، وتسلط الضوء على تدابير حماية الخصوصية، ويقترح الباحث أن تستمر تلك الخصوصية في التطور مستقبلاً، حيث ينظر المستخدمون إلى الخصوصية كأصل شخصي، ويعتمد التحليل على المصادر العلمية لتقديم منظور دقيق وشامل حول انتهاك الخصوصية المتطورة بسرعة.

- استهدفت دراسة (محمد،٢٠٢٢). بعنوان " ***استخدام المراهقين لشبكات التواصل الاجتماعي وعلاقته بإدراكهم لانتهاكات خصوصيتهم***". إلى تسليط الضوء على استخدام المراهقين لشبكات التواصل الاجتماعي بالتطبيق على عينة (٤٥٠) مفردة من المرحلة الثانوية وتحديد أشكال انتهاك الخصوصية والمخاطر التي يتعرض لها هؤلاء المراهقون، واعتمدت منهج المسح الميداني باستبيانات استغرقت مدة شهرين، وتوصلت الدراسة إلى نتائج أن نسبة العينة البحثية ٦١.٧٨% يتابعون شبكات التواصل بشكل دائم، وأن ٤٣.٣٣% يستخدمون المواقع بشكل يومي والابتزاز المادي من أهم أسباب انتهاكات الخصوصية.

- استهدفت دراسة (محمدين،٢٠٢٢). بعنوان " ***اتجاهات النخب نحو تشريعات حماية البيانات عبر مواقع التواصل ودورها في حماية الخصوصية الرقمية لهم***"، حيث منهج الدراسة المسح الميداني للنخب القانونية والأكاديمية ومعرفة التشريعات في مواقع التواصل الاجتماعي، عن طريق استمارة الاستقصاء الإلكترونية بعدد (٥٠) مبحوثاً، والمقابلة شبه المقننة للنخب القانونية والإعلامية بعدد (١٠) مبحوثين، وتوصلت النتائج إلى أن مواقع التواصل الاجتماعي بها عدد من النصوص القانونية التي تمثل الحماية للمستخدمين إضافة إلى إجراءات التحقق من أمان الحساب وارتباطه بالبريد الإلكتروني وأرقام الهاتف المحمول، وفي المقابل فإن سياسية حماية الخصوصية بها بعض الملاحظات والتضارب، مما يجعل

المستخدمين حذرين في كتابة بياناتهم الحقيقية والاستعانة ببيانات وهمية خوفاً من الانتهاكات الرقمية.

- استهدفت دراسة (غريب،٢٠٢١م). بعنوان " ***إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد في ضوء تأثير الشخص الثالث***"، إلى التعرف على تعرض الجمهور لوسائل الإعلام الجديد، ومدى إدراكهم لانتهاك الخصوصية الرقمية، وتأثير العوامل الديموغرافية وتأثير الشخص الثالث مثل المسافة الاجتماعية، وكان منهج الدراسة الوصفية باستخدام أداة الاستبيان الإلكتروني من العينة الميدانية للمجتمع المصري قوامها (٤٣٣) شخص، ومن نتائج المناقشة أتضح أن غالبية المبحوثين مدركين حقوقهم في الخصوصية على وسائل الإعلام الجديد، وأن رد الفعل للجمهور بتنبيه وتحذير أقاربهم بما تعرضوا له من انتهاك للخصوصية، وأيضاَ تأييد الجمهور لفرض رقابة على وسائل الإعلام الجديد ووضع معايير أخلاقية يلتزم بها المستخدمون، ووضع تشريعات تعاقب المخالفين، ومن مقترحات الدراسة الاهتمام بمفهوم التربية الإعلامية من أجل الثقافة والمعرفة للخصوصية الرقمية، وضرورة وضع اليات قضائية لتعزيز الخصوصية الرقمية.

- استهدفت دراسة (إبراهيم،٢٠٢١م). بعنوان " ***الحق في الخصوصية الرقمية في إطار ثورة البيانات وأنماط التدخلات التشريعية والدولية***" إلى تأصيل مفهوم الحق في الخصوصية الرقمية في وجود ثورة البيانات وتحليل الانتهاكات الشخصية والاجتماعية وتحليل الضمانات والمعايير التحويلية، والخصوصية حق من حقوق الإنسان.

- استهدفت دراسة (كدواني،٢٠٢٠م) بعنوان "***ضوابط حماية الحق في الخصوصية عبر مواقع التواصل الاجتماعي***" **إلى** التعرف على مدى الحماية التي توفرها مواقع التواصل الاجتماعي للحق في الخصوصية، حيث تم التحليل الكيفي على

موقعي فيسبوك وإنستغرام لمضمون سياسة الخصوصية على عينة الدراسة. وأثبتت النتائج تشابه الموقعين في سياسة الخصوصية بالتزامهما للمستخدمين والتصريح بجمع المعلومات عنهم، وكيفية استخدامها ومشاركتها ، ويمكن للمستخدمين التحكم في معلوماتهم، وقد خلصت الدراسة إلى أن مواقع التواصل الاجتماعي تملكها شركات تجارية خاصة، تجني أرباحها من جمع بيانات مقابل الخدمات المجانية، ثم تداولها وبيعها إلى طرف ثالث لأغراض مختلفة، وهي التجارة بالبيانات مقابل الخدمة، ويعد هذا العمل انتهاكًا للمستخدمين، و كشفت النتائج أن إعدادات الخصوصية لا تحمي المستخدم ولا تمنع بياناته عن مالكي الخدمة، الأمر الذي يؤكد انعدام الخصوصية المعلوماتية إذ يتوقف الضرر على الأفراد ومقدار مشاركتهم في المواقع، والمعلومات التي يتداولونها مع الآخرين.

٢.٥ محور الهجمات السيبراني :

- استهدفت دراسة (فخرالدين،٢٠٢٣). بعنوان " ***الاتجاهات الحديثة في دراسات مخاطر الإعلام الرقمي*** "، إلى الاهتمام برصد وتحليل وتوصيف الاتجاهات البحثية الحديثة لظاهرة مخاطر الإعلام الرقمي، واعتمدت على منهج التحليل الكيفي والنقدي من المستوى الثاني، وتعد من الدراسات الوصفية التحليلية، وتنوعت الدراسات البحثية وعددها (١٣١) دراسة من الأدبيات العربية والأجنبية، وشملت (٦) اتجاهات من المخاطر في الإعلام الرقمي، ومنها التطرف والفكر الإرهابي، ومخاطر الجرائم الإلكترونية، ومخاطر التأثير على قيم المجتمع وأخلاقياته، وأغلب الدراسات تتناول التأثيرات السلبية على المجتمع، وجاءت نتائج التحليل بأن نظرية الاستخدامات و الإشباعات كانت بالمرتبة الأولى فيما يتعلق بالأطر النظرية المستخدمة، وكان منهجه التحليل والاستبيان في جمع البيانات، وقدمت الدراسة أبعاد مخاطر الإعلام الرقمي ووسائل التواصل الاجتماعي، والتي يجب أن تنطلق منه البحوث المستقبلية.

- كما استهدفت دراسة (المرشد،٢٠٢٣) بعنوان " ***الإعلام الرقمي وجهود مكافحة الإرهاب السيبراني (الدور والمعوقات)*** " إلى التعرف على دور وسائل الإعلام في مكافحة ظاهرة الإرهاب والتطرف خلال الفضاء السيبراني، حيث أصبح الإرهاب الإلكتروني واقعًا على المجتمعات، فالجماعات الإرهابية لم تتوان في الاستثمار والاستغلال في الإعلام الجديد بمختلف تطبيقاته ووسائله، فأصبحت معركة إعلام وصورة ورأي عام ، وإن استخدام تقنية الكمبيوتر والكاميرا هو الأسلوب لكسب الحرب النفسية والدعاية وأفكار الشباب، وتأتي أهمية الدراسة لكيفية توظيف الجماعات الإرهابية للإنترنت والإعلام الجديد بأسلوب الدعاية والتجنيد وجمع الأموال وجمع المعلومات والاتصال الداخلي، وبناء شبكات عالمية من المؤيدين والمناصرين لأفكارهم.

- خلصت دراسة (قرني، خطاب،٢٠٢٢) بعنوان " ***دور مواقع الإعلام الرقمي في حماية الأمن السيبراني***". إلى الوقوف على النمط لميدان الحروب الداخلية والخارجية للهجمات السيبرانية المهددة للأمن القومي للدولة المصرية وكانت مشكلة في دور وسائل الإعلام الرقمي في الحد من الجرائم السيبرانية في مصر؟ وإلي أي مدى يستطيع الإعلام الرقمي مواجهتها؟، ومن الأهداف التعرف على قضايا الأمن السيبراني ورصدها والإمكانيات المتاحة لمواجهة تلك الحروب، حيث تم إجراء دراسة استطلاعية على عينة من صفحات ومواقع الإعلام الرقمي التي تناولت القضايا المتعلقة بالأمن والجرائم السيبرانية، وكانت منهجية الدراسة هي المنهج الوصفي التحليلي والمنهج المقارن، بأداة التحليل الاستراتيجي لرصد نقاط القوة والضعف للمحتوي المقدم في المواقع الخاصة، وأداة تحليل المضمون لتحليل المواقع الخاصة بالأمن السيبراني للتعرف على المعالجة المطروحة للقضية بالأمن السيبراني، ومن التوصيات صياغة مجموعة من الخطط لتحصيل المعلومات والبيانات والحفاظ عليها، وتصنيفها حسب درجات السرية، والتعاون داخل الدولة

بين جميع الهيئات المعنية والقطاعين العام والخاص والشركات العاملة في مجال تكنولوجيا المعلومات من أجل وضع استراتيجية موحدة للأمن الإلكتروني ، وزيادة العقوبات حول جرائم الأمن السيبراني واختراق الحسابات الشخصية أو المؤسسية، ووجود مركز متخصص لاستقبال الشكاوي أو الإبلاغ عن الجرائم السيبرانية، وإنشاء محاكم متخصصة في الجرائم السيبرانية.

٣.٥ محور فقدان الثقة في الأنظمة الرقمية :

- استهدفت دراسة (عمار،٢٠٢٢م). بعنوان " استخدام المراهقين لصفحات مكافحة الجرائم الإلكترونية بالفيس بوك وعلاقته بإدارة خصوصيتهم الرقمية" إلى التعرف على معدل استخدام عينة الدراسة لصفحات مكافحة الجرائم الإلكترونية ودوافع استخدامهم وطرق ادارة الخصوصية لبياناتهم الرقمية ، واعتمدت المنهج الوصفي باستخدام استمارة الاستبيان على عينة عمدية من (٤٠٠) عينة من طلاب الجامعات المصرية من (١٨-٢١) سنة ، وتوصلت الدراسة الى اهتمام العينة باستخدام صفحات مكافحة الجرائم الإلكترونية بالفيس بوك بمعدل مرتفع الى حد ما ، وان دوافع استخدامهم تعزيز قدرتهم على حماية خصوصياتهم ، وتجنب الثغرات التي تسهل انتهاك خصوصياتهم الرقمية ، وان اهتمام الاناث اكثر من الذكور في ادارة البيانات الشخصية والحسابات بمواقع التواصل الاجتماعي بالفيس بوك.

١. واستهدفت دراسة (سيد،٢٠٢١م) بعنوان " ***إدراك مستخدمي مواقع التواصل الاجتماعي لأهمية الأمن السيبراني ودوره في الأمن المعلوماتي*** " إلى دراسة العلاقة بين استخدام مواقع التَّواصل الاجتماعي والإدراك والوعي بأهمية الأمن السيبراني، والحفاظ على أمن المعلومات ، وكان الهدف هو الكشف عن العلاقة بين استخدام مواقع التَّواصل الاجتماعي وإدراك أهمية الأمن السيبراني ودوره في الأمن المعلوماتي، واعتمدت العينة العمدية قوامها (٤٤٠ مُفردة) من مُستخدمي

مواقع التَّواصل الاجتماعي من مختلف الأعمار والمُستويات (التعليمية، الاقتصادية، الاجتماعية)، ومن النتائج، ظهر أن أغلبية (عينة الدِرَاسَةِ) يدركون بالأمن السيبراني وطرق المُحافظة على نظامه بدرجة مُتوسطة ومُرتفعة ، وأيضاً بمخاطره وانتهاكاته بدرجة مُرتفعة ومتوسطة، وأن هناك علاقة ارتباطية دالة إحصائياً بين مُعدلات استخدام مواقع التَّواصل الاجتماعي بهذه المتغيرات (دوافع استخدام مواقع التَّواصل الاجتماعي، وإدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وطرق المُحافظة على نظام الأمن السيبراني، والمخاطر السيبرانية وانتهاكات الأمن السيبراني).

٢. استهدفت دراسة (الغيطي،٢٠٢١)، بعنوان " ***التحديات التي تواجه الصحافة الإلكترونية وسبل معالجتها***" إلى التركيز على معرفة التحديات التي تواجه الصحافة الإلكترونية، وتحديد الجهات المسئولة عن معالجتها، وتستند الدراسة بثلاثة مفاهيم وهي الصحافة الإلكترونية والتحديات والنخب العلمية في ضوء نظرية المسئولية الاجتماعية ونظرية المجال العام، وهي من الدراسات الوصفية، حيث المسح بالعينة العشوائية للنخب العلمية قوامها (٧) مفردات، واعتمدت على المقابلة كأداة جمع المعلومات، واسفرت الدراسة عن مواجهة الصحافة الإلكترونية لمجموعة من التحديات الاقتصادية والتشريعية والتقنية والأمنية التي تؤثر على مستقبلها، وعدم الالتزام بالقوانين والمعايير المهنية التي تواجه الصحافة الالكترونية، وضعف التأهيل والتدريب وانعدام الوعي بالصحافة الالكترونية، ومن أهم الآثار السلبية اعتماد الجمهور على المواقع التفاعلية ووسائل التواصل الاجتماعي وانتشار الشائعات والأخبار المضللة، ومن أهم المقترحات في معالجة التحديات التكيف مع الواقع الاعلامي الحديث والاستعانة بالخبراء في الصحافة الإلكترونية ، وتعميق الرقابة.

٤.٥ التعقيب على الأدبيات :

أفادت الدراسات السابقة الباحث في إيجاد فكرة وصياغة مشكلة وتحديد أهداف الدراسة.

١. جاءت الدراسات بتعبير مدى جدوى وسائل الإعلام الرقمي الحديث على مواجهة ظاهرة الإرهاب السيبراني

٢. وما مدى الخصوصية التي تقدمها وسائل التواصل الاجتماعي للمستخدمين والمحافظة على بياناتهم.

٣. جاءت التوصيات بتكاتف الجهود لجميع الهيئات والشركات والمؤسسات المتضررة بالإرهاب والاختراق السيبراني.

٤. يوضح الباحث أن التطور في تكنولوجيا المعلومات على اتجاهين متعاكسين فبقدر تكثيف الحماية بالأمن السيبراني، بالمقابل يزيد من الاختراقات لوصول التكنولوجيا المعاكسة للخلايا الإرهابية، وأن الانتهاكات والإرهاب السيبراني تؤدي إلى فقدان الثقة في الأنظمة الرقمية.

٦- مشكلة الدراسة :

تنبع مشكلة الدراسة من واقع الانتشار الواسع الذي حققته مواقع التواصل الاجتماعي، وغزوها جميع المجتمعات دون الانتباه والاهتمام لموضوع الخصوصية، فتكمن أساس المشكلة في أن الأفراد أصبحوا يفرطون في خصوصياتهم بوضع معلومات عن أنفسهم أو صورهم الشخصية أو مقاطع فيديو عن مناسبات خاصة بهم وبأسرهم وأصدقائهم على تلك المواقع، التي تكون متاحة للجميع، فأصبحت المعلومات الإلكترونية ملكية عامة بمجرد وضعها في شبكات التواصل الاجتماعي بعد أن كانت ملكية خاصة لصاحبها فقط، ومن ثم تسعى الدراسة لاستكشاف مدى الحماية التي

توفرها المنصات الاجتماعية للحق في الخصوصية، والوعي بكيفية استخدام مواقع التواصل الاجتماعي والحفاظ على المعلومات الشخصية، وكيف يمكن للشركات والهيئات مواجهة حالات الاختراق السيبراني للأنظمة التي تهدف إلى سرقة البيانات أو تعطيل الخدمات الرقمية والعمليات الحيوية والاقتصادية ، فإن انتهاك خصوصية الأخرين والتدخل في حياتهم الشخصية وحريتهم دون أدنى اعتبار، الأمر الذي له انعكاسات سلبية على من يتم التعدي على بياناته ، ويؤثر سلبًا على نواحٍ عديده منها التسلط وفرض الهيمنة على الخصوصية من خلال نشر معلومات أو صور أو بعض من الأسرار الشخصية ، والتحكم من قِبلِ الأشخاص الخطأ ونعني بها (الابتزاز)، ولذلك نحتاج أن نتعلم كيفية احترام خصوصية الأخرين ، فنحتاج أن ننشئ جيلاً يعي أن حريته تبدأ من احترام الخصوصية ، ونحتاج التركيز على ثقافة الاستئذان وأن نطرق الباب ويؤذن لنا قبل الدخول، ويمكن صياغة المشكلة الرئيسية، ماهي التحديات والمخاطر وفقدان الثقة الإعلامية في ظل الإعلام الرقمي في محاور (انتهاك الخصوصية، والهجمات السيبرانية، وفقدان الثقة في الأنظمة الرقمية)، وبقدر انتهاك الخصوصية والهجمات السيبرانية التي تفقد ثقة المستخدمين في الأنظمة الرقمية.

٧- أسئلة الدراسة :

١. ما هي الآثار المحتملة للهجمات السيبرانية على الأفراد والمؤسسات التي تواجه التقدم التكنولوجي في الإعلام الرقمي؟

٢. كيف يمكن تعزيز حماية البيانات الشخصية في ظل التهديدات السيبرانية المتزايدة؟

٣. ما تصور الشركات والمؤسسات في تعزيز استراتيجيات أمن المعلومات للحد من التهديدات السيبرانية؟

٤. ما وسائل توعية الجمهور بأهمية حماية الخصوصية الرقمية وتقليل المخاطر التكنولوجية في الإعلام الرقمي؟

٥. كيفية قياس فعالية التدابير الأمنية المتخذة في مواجهة التهديدات السيبرانية في البيئة الرقمية؟

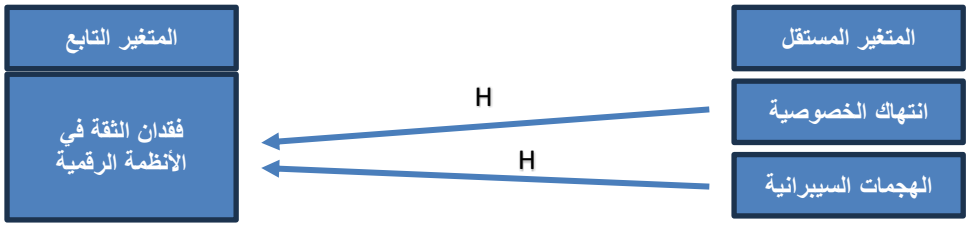
٨- أهداف الدراسة :

لدراسة البحث بعنوان "التحديات والمخاطر وفقدان الثقة الإعلامية في ظل الإعلام الرقمي وانتهاك الخصوصية والهجمات السيبرانية" تشمل:

١. معرفة تأثير الهجمات السيبرانية على الأفراد والمؤسسات وتحليل ودراسة التحديات بفهم مخاطر انتهاك الخصوصية التي يواجهها التقدم التكنولوجي والتصدي لها في مجال الإعلام الرقمي والبيئة الرقمية الحالية.
٢. استكشاف أهمية التوعية بأمن المعلومات وسبل تعزيز الوعي الرقمي لدى الجمهور والعاملين في هذا المجال.
٣. تقييم السياسات والتشريعات الحالية المتعلقة بحماية الخصوصية وتقديم مقترحات لتعزيزها وتحسينها.
٤. تحليل دور الأمن السيبراني والتقنيات الحديثة في حماية البيانات وتقديم استراتيجيات لتحسين أمن المعلومات.
٥. قياس فعالية التدابير الأمنية المتخذة وتقييم أثرها على تقليل التهديدات السيبرانية وحماية البيانات بشكل فعال.
٦. التوصل إلى مجموعة من التوصيات في ضوء ما سيتم التوصل إليه من النتائج التي سوف يتم الحصول عليها بحيث يمكن تطبيقها والاستفادة منها.

٩- نموذج الدراسة

يوضح النموذج التالي متغيرات الدراسة ويشمل انتهاك الخصوصية، والهجمات السيبرانية كعوامل مستقلة، والمتغير التابع تتمثل في فقدان الثقة الإعلامية في الأنظمة الرقمية، كما يظهر في الشكل التالي:



الإطار المقترح لنموذج الدراسة

١٠- فرضيات الدراسة :

١. يوجد تأثير ذو علاقة ارتباطية معنوية ذات دلالة إحصائية بين انتهاك الخصوصية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي.

٢. يوجد تأثير ذو علاقة ارتباطية معنوية ذات دلالة إحصائية بين الهجمات السيبرانية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي.

١١- أهمية الدراسة :

إن دراسة التحديات والمخاطر وفقدان الثقه الإعلاميه التي تنشأ نتيجة التقدم التكنولوجي في ظل الإعلام الرقمي هي ذات أهمية كبيرة، خاصة فيما يتعلق بحماية الخصوصية والتصدي للهجمات السيبرانية التي تعد أمورًا حيوياً لضمان استدامة وأمان البيئة الرقمية التي تعترض طريق التقدم التكنولوجي، وفقدان الثقة الإعلامية.

١.١١ الأهمية العلمية (النظرية)

يترافق التقدم التكنولوجي الابتكار وتبادل المعرفة والمعلومات مع تحديات ومخاطر متنوعة تتعلق بالخصوصية والأمن السيبراني. إلى أهمية عمل الباحثين والمتخصصين في دراسة وفهم التحديات والمخاطر التي تنشأ عن التقدم التكنولوجي في الإعلام الرقمي، وتطوير السياسات والإجراءات اللازمة للتعامل معها بشكل فعال ومستدام.

١. تحديد نقاط الضعف في أنظمة الحماية حيث أن التقدم التكنولوجي يجعل جمع المعلومات أكثر سهولة، ولكنه في الوقت نفسه يتسبب في تزايد خطر انتهاك الخصوصية.

٢. وضع إستراتيجيات للوقاية من التسريب والاستخدام غير القانوني. حيث أن التقدم التكنولوجي يجلب ثغرات أمنية جديدة وتهديدات سيبرانية متطورة.

٣. تسليط الضوء على ضرورة وضع سياسات وقوانين لضمان أمان البيانات وحقوق الأفراد والشفافية.

٤. كيفية تأثير واستخدام التكنولوجيا الرقمية على الثقافة والهوية والتفاعلات الاجتماعية على السلوك البشري.

٥. دراسة للقيم والأخلاقيات المتعلقة بالاستخدام المتزايد للتكنولوجيا وتأثيرها على الخصوصية والحقوق.

٦. تعزيز الوعي الرقمي لدى المشاركين في المحتوى الرقمي بفهم أهمية حماية البيانات والمعلومات الشخصية عند التفاعل مع الإعلام الرقمي وجعلهم أكثر قدرة على التعرف على التهديدات والتصدي لها.

٧. استغلال فوائد التقدم التكنولوجي في الإعلام الرقمي لإدارة المخاطر وحماية الخصوصية والأمن السيبراني.

٢.١١ الأهمية العملية (التطبيقية)

١. التهديدات السيبرانية وانتهاك الخصوصية تشكل خطرًا كبيرًا على الأعمال والمؤسسات، فتساعد الدراسة صناع القرار بفكرة وضع تشريعات جديدة تضمن حماية بيانات المستخدمين في مواقع التواصل الاجتماعي.

٢. يتطلب التقدم التكنولوجي استخدام تقنيات حماية متقدمة واستخدام حلول الأمن السيبراني.

٣. من خلال توفير التدريب والتوعية بالأمن السيبراني للنظم والتطبيقات الرقمية، معرفة كيفية تطبيق معايير عالية للأمان وحماية البيانات.

٤. الابتكار في مجال الأمن السيبراني، وتطوير حلول جديدة وفعالة للتعامل مع التهديدات السيبرانية المتزايدة، وتطوير تقنيات وأدوات جديدة لتعزيز الأمن السيبراني وحماية البيانات.

١٢- مفاهيم ومصطلحات الدراسة :

١.١٢ التحديات والمخاطر :

التحديات: تشير إلى الصعوبات التي تواجه عمليات الإعلام الرقمي والتكنولوجيا الرقمية بشكل عام (الغيطي،٢٠٢١). أما **المخاطر:** تشير إلى الأضرار أو الخطر التي تتسبب فيها تقنيات الإعلام الرقمي.

وكما عرفه الباحث فإن **التحديات والمخاطر** في الإعلام الرقمي هي الصعوبات والأخطار التي تنشأ نتيجة التقدم التكنولوجي واستخدام التقنية الرقمية في العمليات الإعلامية.

***وأضاف الباحث بتعريفه أن* التحديات والمخاطر** هي قدرة الأفراد على فهم الأخبار والمعلومات عبر وسائل الإعلام الرقمي، وتأثيرها على وعيهم واستيعابهم للمحتوى الرقمي.

٢.١٢ فقدان الثقة الإعلامية :

هو عدم قدرة الإعلام الرقمي على إقناع الجمهور بنقل الأخبار والآراء لما فيها من أخبار مزورة تشوه الحقائق. (شومان،٢٠١٧م)

وقد عرفه الباحث بأنه الاعتماد والاستيعاب بدقة المعلومات في مواقع التواصل الاجتماعي التي قد تكون مضللة ومصنوعة بتطبيقات الذكاء الاصطناعي.

٣.١٢ الإعلام الرقمي :

عرفه الباحثون بأنه وسائل الإعلام التي تعتمد على التكنولوجيا بالصوت والصورة والكتابة الرقمية الحاسوبية ويشير إلى استخدام التقنية الرقمية في العمليات المتعلقة بالاتصال والإنتاج والتوزيع وتبادل المعلومات. (عثمان،٢٠٢٣م).

كما عرفه الباحث بكيفية التفاعل بين المستخدمين مع المحتوى الرقمي واستيعابهم للمعلومات وإبداع أفكارهم باستخدام التكنولوجيا الرقمية والإنترنت والشبكات الاجتماعية والتطبيقات الرقمية للتواصل ونقل المعرفة.

٤.١٢ انتهاك الخصوصية :

هو انتهاك حق الفرد في حماية معلوماته الشخصية والحفاظ على خصوصيته ومراقبته بدون وجه حق. (غريب،٢٠٢١م)

كما عرفه الباحث بانتهاك حق الإنسان في المحافظة على سرية تداول معلوماته ومراقبته وتتبعه عبر الوسائط الرقمية.

٥.١٢ الهجمات السيبرانية :

هي الهجمات التي تتم عبر الإنترنت أو شبكات الكمبيوتر، وتهدف إلى الاختراق غير المشروع لأنظمة المعلومات أو البيانات أو البرامج.

كما عرفه الباحث بالتهديدات والهجمات التي تتعرض لها البيانات والأنظمة الرقمية والاستخدام غير القانوني للمعلومات من سرقة وتلاعب البيانات لتشويه الدراسات والنتائج العلمية.

١٣- الجانب الفكري والعلمي للدراسة :

خلال ربع قرن من الزمان وفي مجال اختصاص الباحث في تقنية المعلومات من برمجة باللغات المختلفة وتشغيل الحاسبات الكبيرة المين فريم وصولا إلى تأسيس الشبكات بأنواعها، ومن خبرات متنوعة في تصميم المواقع الإلكترونية ومن لجان الرقمنة والتحول الرقمي، لخص الباحث أفكاره ووضعها بين أيديكم بمفاهيم التقنية، وحيث لانتهاك الخصوصية الكثير من الأشكال والأساليب، وهو التدخل غير المشروع في الحياة الشخصية للآخرين دون موافقتهم، وينتج عن ذلك وضع الآخرين بتجارب ومواقف محرجة أو إجبارهم على التعامل مع أشخاص رغماً عنهم.

١.١٣ هل يشكل الإنترنت تهديدًا للخصوصية؟

قد يتم استخدام أي معلومات تضعها على الشبكة العنكبوتية بشكل ضار ويمثل تهديداً للخصوصية بسبب عدة عوامل:

١. كثير من الشركات والمنظمات تقوم بجمع البيانات عبر الشبكة العنكبوتية، ومن الصعب معرفة كيفية استخدام هذه البيانات ومن يمكن الوصول إليها.

٢. هذه البيانات تتيح للشركات تتبع نشاط المستخدمين عبر الشبكة العنكبوتية، وبواسطة خوارزميات مبرمجة تنتهي بعرض إعلانات مستهدفة مما يشكل انتهاكاً للخصوصية.

٣. الاختراقات السيبرانية وسرقة البيانات الشخصية والمالية يعرض خصوصية المستخدمين للخطر ويمثل تهديداً للشركات والهيئات الحكومية والأفراد.

٤. قد لا يكون المستخدمين مدركين بأهمية حماية خصوصياتهم عبر الشبكة العنكبوتية بنقص الوعي مما يؤدي إلى تعرضهم للتهديدات.

(موقع كاسبر سكاي)

٢.١٣ أخلاقيات الإعلام الرقمي :

الإعلام الرقمي يشكل مجموعة من المبادئ والقيم التي تحدد كيفية استخدام التكنولوجيا الرقمية بشكل أخلاقي ومسؤول. ويعمل على توجيه السلوك والتفاعلات الاجتماعية، كما يعزز الاحترام المتبادل والشفافية والمسؤولية الفردية والجماعية، ومن الأخلاقيات:

١. التعامل مع بيانات المستخدمين بسرية، واحترام الخصوصية، وعدم جمع المعلومات الشخصية إلا بموافقة صريحة.

٢. التعامل مع المعلومات بشفافية وصدق، وتجنب نشر المعلومات المضللة أو الكاذبة.

٣. مراعاة المحتوى المنشور بمسؤولية وعدم إثارة الكراهية أو العنف أو الضرر للأفراد والمجتمعات، والحفاظ على الموضوعية والتوازن في العرض والتقديم.

٤. توفير محتوى متنوع وشامل يعكس تنوع المجتمع، وعدم التمييز بناءً على العرق، أو الدين، أو الجنس، أو العمر، أو الإعاقة، أو أي صفات أخرى.

٥. احترام حقوق الملكية الفكرية وعدم استخدام المحتوى دون إذن من أصحابه.

٦. اتخاذ التدابير اللازمة لحماية الأنظمة والبيانات من الهجمات السيبرانية وسلامة الخدمات الرقمية.

٧. تشجيع التفاعل الإيجابي وبناء المجتمعات الرقمية الراقية، وتجنب التحريض عبر منصات وسائل التواصل الاجتماعي.

٨. تعزيز التوعية بأخلاقيات الإعلام الرقمي لدى المستخدمين واتخاذ القرارات الصحيحة والمسؤولة.

(المجدوب،٢٠١٩).

٣.١٣ التقدم التكنولوجي في الاعلام الرقمي :

إن مفهوم التطورات والابتكارات التكنولوجية هي كيفية إنتاج وتوزيع واستهلاك المحتوى الإعلامي، وتشكل طريقة تفاعلنا مع المعلومات والمحتوى الإعلامي في عصرنا الرقمي. تطور وسائل الاتصال التكنولوجية مثل الإنترنت والهواتف الذكية ووسائل التواصل الاجتماعي أدى إلى توفير قنوات وأساليب جديدة للوصول إلى المعلومات والتفاعل الاجتماعي. فظهرت تقنيات جديدة لإنشاء وتوزيع المحتوى الرقمي بمختلف الأشكال، مثل الصور والفيديوهات والتطبيقات التفاعلية وخدمات البث المباشر.

١. يساعد الذكاء الاصطناعي وتحليل البيانات على فهم السلوكيات والاهتمامات للمستخدمين بشكل أفضل، وتخصيص المحتوى وتوجيه الإعلانات واستهدافه بشكل أكثر دقة وفعالية.

٢. تقنيات الواقع الافتراضي والواقع المعزز تفتح أبوابًا جديدة لتجارب الوسائط الرقمية التفاعلية.

٣. البث المباشر والفيديو عند الطلب يوفران للمستخدمين مرونة أكبر في مشاهدة المحتوى في أي زمان ومن أي مكان.

٤. تطورت تقنيات التخزين الرقمي و السحابي لتوفير وصول سهل وآمن إلى المحتوى والبيانات عبر الشبكة العنكبوتية. (حاجة،٢٠٢٣م).

٤.١٣ مفهوم السحابة والتخزين الرقمي :

إن هذا المفهوم يتعلق بتقنية تخزين البيانات والملفات عبر الإنترنت في بيئة سحابية، وهي مساحة افتراضية على أجهزة بعيدة والمتواجدة في مراكز متخصصة بدلاً من استخدام موارد على أجهزة الكمبيوتر الشخصية، وأهم ميزة للتخزين الرقمي السحابي هي القدرة على الوصول إلى البيانات والملفات من أي مكان وفي أي زمان، بشرط توفر الاتصال بالإنترنت، كما يجب النظر في سياسات مقدم الخدمة قبل الاستخدام وتشمل:

١. تخزين البيانات: حيث تقدم مساحة تخزين على الإنترنت لحفظ البيانات والملفات بأمان وكفاءة عالية مثل (Dropboxو Google Drive).

٢. حوسبة السحابة: توفر المعالجات لتشغيل التطبيقات ومعالجة البيانات.

٣. النسخ الاحتياطي واستعادة البيانات: تقدم القدرة على إجراء نسخ احتياطية للبيانات تلقائياً بواسطة بعض البرامج مثل (Carbonite) واستعادتها عند تعطل أجهزة الكمبيوتر.

٤. مشاركة الملفات: تمكن مشاركة الملفات والمستندات بسهولة مع الآخرين عبر الإنترنت وتحريرها.

٥. الأمان والحماية: توفر آليات حماية وأمان متقدمة للبيانات تضمن سلامتها وسرية محتواها.

(مثابر،٢٠٢٤م).

٥.١٣ مفهوم الأمان والحماية في الإعلام الرقمي :

وهو الجهد والتدابير التي يتخذها الأفراد والمؤسسات لحماية بياناتهم ومعلوماتهم والأنظمة الرقمية من التهديدات والهجمات السيبرانية والاختراقات والمخاطر الأمنية.

١. التشفير: يتم استخدام التشفير لحماية البيانات والتأكد من سلامتها، مما يمنع التلاعب والتجسس على البيانات.

٢. إدارة الهوية والوصول: يتم منح الوصول إلى البيانات والأنظمة الرقمية للأشخاص المخولين فقط وبطرق آمنة، ويشمل استخدام تقنيات التحقق الثنائي.

٣. الحماية من البرمجيات الخبيثة: يتطلب استخدام برامج مكافحة الفيروسات والبرمجيات الضارة وتحديثها بانتظام للحماية من الهجمات السيبرانية.

٤. التدريب والتوعية: لابد من تدريب وتوعية المستخدمين حول كيفية التعامل مع المخاطر الرقمية، والتحذير من التصيد الاحتيالي والهجمات السيبرانية.

٥. حماية الخصوصية: يجب حماية خصوصية البيانات الشخصية وعدم تسربها أو استخدامها بشكل غير قانوني.

٦. التحقق والمراقبة: تفعيل أنظمة مراقبة وتحليل السجلات للكشف عن نشاط غير مصرح به، أو مشبوه باتخاذ الإجراءات الضرورية.

٧. الخطط والإستراتيجيات: وضع خطط إستراتيجية للتعافي من الاختراقات الأمنية بسرعة وفعالية للحد من الأضرار. (الشامسي،٢٠٢٣م).

٦.١٣ مفهوم البرمجيات الخبيثة :

البرمجيات الخبيثة (Malware) هي برمجيات يتم تطويرها بغرض الإضرار للأنظمة الحاسوبية والمستخدمين، وتقوم بسرقة البيانات أو إتلافها أو حذفها،

وأيضاً التجسس على المستخدم، ويتم انتشار البرمجيات الخبيثة عبر الإنترنت، من خلال التنزيلات غير الآمنة، أو رسائل البريد الإلكتروني الاحتيالية، أو الروابط الضارة. لذلك، من الضروري استخدام برامج مكافحة الفيروسات والبرمجيات الأمنية واتخاذ التدابير الوقائية لحماية الأنظمة والبيانات من الهجمات الخبيثة، ومن أشكال هذه البرامج:

١. الفيروسات (Viruses): تعد الفيروسات من أنواع البرمجيات الخبيثة، وتعمل عند تشغيل الملفات المصابة، حيث تقوم بنسخ نفسها والانتشار إلى ملفات أخرى في النظام.

٢. برامج التجسس (Spyware): تستخدم لمراقبة وجمع المعلومات عن أنشطة المستخدم على الحاسوب دون علمه، بسرقة كلمات المرور وكلمات البحث وتاريخ التصفح ومعلومات تسجيل الدخول، ويتم إرسال هذه المعلومات إلى مرسلي برمجيات التجسس دون علم المستخدم.

٣. برامج الفدية (Ransomware): تعمل هذه البرامج على تشفير ملفات المستخدم ومن ثم مطالبته بدفع فدية مالية لاستعادة الملفات.

٤. أحصنة طروادة (Trojans): تسكن هذه البرمجيات بين ملفات النظام وعند تفعيلها تقوم بتنفيذ أنشطة خبيثة.

٥. برامج الاعلانات (Adware): هو عرض إعلانات وقد تقوم بجمع معلومات عن حركة تصفح المستخدمين.

٦. بوتنت (Botnets): تعتبر بوتنت من البرمجيات التي يتم التحكم بها عن بعد من قبل المهاجمين، للتحكم في حاسوب الطرف الآخر.

٧. برامج التتبع (Tracking software): تستخدم لجمع بيانات حول سلوك المستخدمين على الإنترنت، وحركاتهم في المواقع والإعلانات وتستخدم هذه البيانات في توجيه الإعلانات المستهدفة.

٨. برامج الاختراق (Malware): وتهدف إلى التسبب في أضرار لأجهزة المستخدمين أو سرقة معلوماتهم الحساسة.

٩. برامج الاعتراض الرجعي (Keyloggers): تسجل الضغطات على لوحة المفاتيح (حركة لوحة المفاتيح) بدون علم المستخدم، مما يتيح معرفة وسرقة المعلومات الحساسة، مثل بيانات تسجيل الدخول وكلمات السر.

١٠. برمجيات الاحتيال (Scareware): وهو إقناع المستخدمين بأنهم مصابون بالفيروسات أو البرمجيات الخبيثة وتحثهم على شراء برنامج أمان غير موثوق به.

١١. الديدان (worms): برامج قادرة على استنساخ نفسها إلى حواسيب أخرى على نفس الشبكة.

١٢. التصيد الإلكتروني (phishing) .ويستعين التصيّد هذا برسائل البريد الإلكتروني والمواقع الإلكترونية الاحتيالية المصممة لسرقة الهويات والبيانات الشخصية.

(سايبر أرابز،٢٠١٧).

٧.١٣ مفهوم الخوارزميات في الإعلام الرقمي :

تُستخدم الخوارزميات لتنظيم وتحليل البيانات والعثور على المعلومات وحركة المستخدم في الشبكة العنكبوتية في الإعلام الرقمي:

١. تحليل البيانات والتنبؤ التي تُولد عبر منصات الإعلام الرقمي مثل مواقع التواصل الاجتماعي ومواقع الويب، لفهم سلوك المستخدمين وتوجيه الإعلانات

الإعلامية والتسويقية المستهدفة، كما تنبأ بالاتجاهات والأنماط المستقبلية بناءً على البيانات التاريخية.

٢. تخصيص التجربة الإعلامية، والمحتوى الإعلامي، والإعلانات لكل مستخدم بناءً على اهتماماته وسلوكه السابق عبر الشبكة العنكبوتية. فيزيد من فعالية الإعلانات والمحتوى.

٣. التصنيف والتصفية للمحتوى الرقمي، لعرض أفضل المحتويات للمستخدمين أو لمكافحة انتشار المحتوى الضار.

٤. التحكم في الترتيب والأولويات في عرض المحتوى عبر منصات الإعلام الرقمي، كترتيب النتائج في محركات البحث بناءً على عوامل التفاعل.

٥. التعلم الآلي والذكاء الاصطناعي في الإعلام الرقمي يتيح لها التكيف مع التغيرات وتحسين أدائها بمرور الوقت.

(المراقب،٢٠٢٣).

٨.١٣ مفهوم التفاعل مع الجمهور في الإعلام الرقمي :

مواقع التواصل الاجتماعي، والمدونات، والمنتديات، والتطبيقات الرقمية، هذا التفاعل مع الجمهور في الإعلام الرقمي، وهو تواصل المحتوى الرقمي مع جمهورهم عبر الوسائط الرقمية وهو جزء من استراتيجيات التسويق وإدارة المحتوى الرقمي تساهم في بناء علاقات قوية.

١. الردود والتعليقات على المنشورات والمقالات والفيديوهات ومحتويات العالم الرقمي، يتيح للمشاركين التعبير عن آرائهم وتقديم ملاحظاتهم.

٢. المشاركة والنشر للمحتوى يساهم في زيادة انتشار المحتوى لفئات أوسع من الجمهور.

٣. التصويت والاستطلاعات عبر الإعلام الرقمي لجمع آراء الجمهور والتفاعل معها.

٤. الجلسات الحوارية حيث يتم مناقشة مواضيع محددة وتبادل الآراء والأفكار.

٥. الاستفسارات وطلب الدعم والمساعدة من مقدمي المحتوى، ويتم تقديم الردود والمساعدة عبر الوسائط الرقمية والدردشات الحية والرسائل الفورية.

٦. التفاعل مع العلامات التجارية والشركات عبر التعبير عن اهتمامهم بالمنتجات أو الخدمات، وتقديم الملاحظات والتعليقات.

٧. التفاعل مع المحتوى الخاص الذي يتم نشره عبر وسائل التواصل الاجتماعي، مثل الصور والفيديوهات والقصص.

٨. التفاعل مع المجتمعات والمجموعات ذات الاهتمامات المشتركة عبر وسائل التواصل الاجتماعي، يتيح تبادل المعلومات الثقافية والمعرفية.

٩.١٣ مفهوم التعلم الآلي والذكاء الاصطناعي في الإعلام الرقمي :

التعلم الآلي والذكاء الاصطناعي في الإعلام الرقمي باستخدام تقنيات تحليل البيانات وتحسين تجربة المستخدم وتقديم المحتوى بشكل أكثر فعالية وخصوصًا:

١. التعلم الآلي (Machine Learning): هو فرع من الذكاء الاصطناعي لتحليل البيانات واكتشاف الأنماط والاتجاهات وتوقع السلوك المستقبلي للمستخدمين، دون تدخل البرمجة البشرية، (أوراكل،)

٢. الذكاء الاصطناعي (Artificial Intelligence): إنشاء أنظمة تكنولوجية تظهر سلوكًا يماثل الذكاء البشري، لأداء المهام مع تطوير نفسه بشكل دوري، (اوراكل،)

يمكن الاستفادة منهما في الإعلام الرقمي بالطرق التالية:

– استخدام التعلم الآلي لتحليل سلوك المستخدمين وتخصيص وتقديم محتوى مناسب لكل فرد.

– تحسين تجربة المستخدم عبر تحليل السلوك والاستجابة الفورية لاحتياجاتهم وتفضيلاتهم.

– توجيه واستهداف العمليات الإعلانية باستخدام الذكاء الاصطناعي بناءً على تحليل البيانات السلوكية للمستخدمين.

– تحليل البيانات والاتجاهات باستخدام التعلم الآلي واكتشاف الأنماط والاتجاهات وتوقع المستقبل.

– استخدام تقنيات الذكاء الاصطناعي لفهم وتحليل اللغة الطبيعية والمشاركات على وسائل التواصل الاجتماعي. (أوراكل،)

١٠.١٣ مفهوم GPS في الإعلام الرقمي :

هو نظام تحديد المواقع العالمي (Global Positioning System) "GPS" ، يستخدم لتحديد المواقع في الهواتف الذكية والسيارات والطائرات والسفن لتحديد الزمان والمكان على سطح الأرض بدقة، ويعتمد على شبكة من الأقمار الصناعية تدور حول الأرض وترسل إشارات إلى جهاز GPS لحساب موقعه بالنسبة للأقمار الصناعية، ومن استخداماتها:

١. تطبيقات الخرائط والملاحة، تستخدم GPS لتوفير الاتجاهات والمسارات الأمثل أثناء القيادة، وتوفير معلومات حول المواقع والخدمات القريبة.

٢. تتبع المركبات، يستخدم GPS في تتبع المركبات التجارية، مما يتيح معرفة مواقع المركبات ومراقبتها من قبل الشركات المملوكة لها.

٣. الأنشطة الرياضية والترفيهية، يستخدم GPS في تطبيقات تتبع الأنشطة الرياضية، وألعاب الهواتف الذكية التي تعتمد على المواقع.

٤. الأمن الشخصي، يستخدم GPS في تطبيقات الأمن الشخصي، وتطبيقات إرسال الموقع للطوارئ.

٥. التسويق المحلي، يستخدم GPS لتوجيه الإعلانات التجارية والعروض الترويجية إلى المستهدفين بناءً على مواقعهم الجغرافية، مما يزيد فعالية الإعلانات والتسويق المحلي. (فاستر كابيتال،٢٠٢٤).

١١.١٣ طرق معرفة البرامج الخبيثة في الإعلام الرقمي :

توجد عدة طرق للكشف عن البرامج الخبيثة في الإعلام الرقمي ومنها:

١. برامج مكافحة الفيروسات والتي تعمل على مسح الأجهزة والكشف عن البرامج الضارة وتنظيفها.

٢. التحديثات الأمنية والتي تعمل على سد الثغرات الأمنية التي يمكن استغلالها من قبل البرامج الضارة.

٣. استخدام الحماية التي توفر فلترة البريد الإلكتروني والمرفقات والروابط للتحقق من خلوها من البرمجيات الخبيثة.

٤. استخدام برامج الفحص التي تقدمها بعض الشركات المتخصصة في كشف البرمجيات الخبيثة عبر الإنترنت.

١٢.١٣ فهم تأثير التكنولوجيا على المجتمع والفرد :

إن فهم تأثير التكنولوجيا على المجتمع والفرد يتطلب التفكير في العديد من الجوانب المختلفة ومنها:

١. غيرت التكنولوجيا كيفية التواصل والتفاعل الاجتماعي في الحياة الاجتماعية، حيث أصبحت وسائل التواصل الاجتماعي جزءاً من حياة الناس. مما أدي إلى تغيير أنماط العلاقات الاجتماعية.

٢. إن استخدام التكنولوجيا الرقمية والإنترنت بشكل مفرط يؤثر على الصحة العقلية والنفسية، مثل انعدام النوم والشعور بالوحدة والعزلة بسبب التفاعل الاجتماعي عبر الإنترنت.

٣. توجد تأثيرات كثيرة على الاقتصاد والعمل حيث جعلت التكنولوجيا العديد من الوظائف تتغير أو تتلاشى، وبالمقابل أنشأت وظائف رقمية جديدة متعلقة بالتطورات التكنولوجية.

٤. من خلال وسائل التواصل الاجتماعي أصبح الوصول إلى المعلومات والمصادر التعليمية المجانية بسهولة. حيث التأثير في تحسين الحالة الاجتماعية والاقتصادية للأفراد والمجتمعات.

٥. حدثت تحولات في الأعمال والصناعات بسبب تقنيات الذكاء الاصطناعي والتعلم الآلي في مجال العمل والإنتاج والإعلام، وأثرت على الصناعات حيث يتطلب تطوير مهارات جديدة.

٦. يتعين على المجتمعات التوازن بين الفوائد والتحديات والاستفادة من التكنولوجيا بالأسلوب الإيجابي ومواجهة التحديات التي قد تطرأ بأسلوب سلبي، مثل انعدام الخصوصية والاعتماد المفرط على التكنولوجيا.

١٣.١٣ تأثير الهجمات السيبرانية على الاقتصاد والدول في الإعلام الرقمي :

الهجمات السيبرانية تؤثر بشكل كبير على الاقتصاد في الإعلام الرقمي من عدة طرق:

١. تتسبب الهجمات السيبرانية في خسائر إصلاح الأضرار الناتجة عن الهجمات وفقدان البيانات الحساسة والملكية الفكرية وصعوبة استعادة البيانات المفقودة أو تعويض العملاء عن الأضرار.

٢. تؤدي الهجمات السيبرانية إلى فقدان الثقة لدى العملاء والمستخدمين في الشركة المتضررة، مما يؤدي إلى فقدان العملاء والإيرادات المستقبلية، وانكماش اقتصادي

٣. تؤدي الهجمات السيبرانية إلى توقف الخدمات الحيوية والبنية التحتية مما يتسبب في خسائر مالية فورية وتأثيرات سلبية على الإنتاجية.

٤. تؤدي الهجمات السيبرانية إلى تراجع الاستثمارات وتهديد للأمن والاقتصاد الوطني بشكل عام، وتشكل تأثيرات سلبية على الاقتصاد في الإعلام الرقمي من خلال تعطيل الأنظمة المالية أو سرقة المعلومات الحساسة أو تعطيل الإنتاجية الاقتصادية، ويبين أهمية اتخاذ التدابير الأمنية وتعزيز الوعي للوقاية من هذه التهديدات.

٥. التأثير على السياسة والعلاقات الدولية بسبب الهجمات السيبرانية جزء من التوترات وقد تسبب في التصعيد بين الدول.

٦. التأثير على الثقة العامة في قدرة الدول على حماية بياناتهم الذي يؤثر على استقرار الحكومة والاستقرار الاجتماعي.

٧. التأثير على الحوكمة الرقمية فقد تضطر الدول إلى اتخاذ إجراءات قوية لتعزيز الأمن السيبراني وتطوير سياسات الحوكمة الرقمية الذي يتطلب استثمارات مالية هائلة وتغييرات هيكلية.

٨. (سكاي نيوز عربية،٢٠٢٣).

١٤.١٣ تأثير الهجمات السيبرانية على الأفراد في الإعلام الرقمي :

من بين هذه التأثيرات:

١. الهجمات السيبرانية تؤدي إلى فقدان وسرقة البيانات الشخصية للأفراد، مثل المعلومات الشخصية وبيانات الحسابات المصرفية والمعلومات الطبية الذي يتسبب في انتهاك خصوصية والمخاطر المالية.

٢. قد تستخدم البيانات المسروقة في عمليات الابتزاز الرقمي، حيث يطالب المهاجمون بمبالغ مالية مقابل عدم نشر المعلومات الشخصية، واستخدامها في عمليات احتيالية.

٣. تتسبب الهجمات السيبرانية في تأثير عقلي ونفسي على الأفراد نتيجة خسارة البيانات أو التعرض للابتزاز الرقمي.

٤. من الطبيعي أن التعرض للهجمات السيبرانية يؤدي إلى فقدان الثقة لدى الأفراد في استخدام الإنترنت وتقنياته، فيؤثر على نمط حياتهم واعتمادهم على الخدمات الرقمية.

٥. تدمير العلاقات الاجتماعية بين الأفراد وفقدان الثقة في التفاعلات الاجتماعية.

١٥.١٣ الإعلانات التسويقية والخوارزميات في الإعلام الرقمي :

تعتمد الإعلانات التسويقية في الإعلام الرقمي على استخدام الخوارزميات لتحسين استهداف الجمهور وتحقيق أقصى قدر من التفاعلية:

١. استهداف الجمهور: تستخدم الخوارزميات في تحليل البيانات الضخمة لفهم سلوكيات الجمهور على الإنترنت، واستهداف الإعلانات بشكل دقيق للفئات العمرية المستهدفة والمهتمة بالمنتجات المحددة.

٢. التحسين المستمر: تستخدم الخوارزميات تقنيات التعلم الآلي والذكاء الاصطناعي لتحسين أداء التسويق الإعلانية باستمرار.

٣. تخصيص الإعلانات التجارية، تساعد الخوارزميات في تخصيص الإعلانات التجارية لكل زائر بناءً على اهتماماته وسلوكياته السابقة على الإنترنت.

٤. تحليل الأداء: تستخدم الخوارزميات لتحليل أداء الإعلانات والمبيعات وقياس النتائج بدقة، وتحديد الإعلانات الأكثر فاعلية.

٥. تحسين تجربة المستخدم: تساعد الخوارزميات في تحسين تجربة المستخدم (UX) عبر محتوى وتطبيقات تسويقية. (مركز القرار للدراسات الإعلامية،٢٠٢٣).

١٦.١٣ أشكال وأساليب انتهاكات الخصوصية :

١. جمع البيانات الشخصية للأفراد دون الحصول على موافقتهم أو علمهم.

٢. مشاركة البيانات الشخصية التي تم جمعها مع أطراف ثالثة دون علم أو موافقة الأفراد.

٣. اختراق البيانات والنظام المعلوماتي واستخدام هذه البيانات في أنشطة غير مشروعة.

٤. استخدام التقنيات الرقمية لتتبع وتعقب الأفراد دون علمهم، عبر متصفح الإنترنت، والتطبيقات، وأنظمة الجوال.

٥. انتهاك الخصوصية لتوجيه الإعلانات التجارية والعروض التسويقية بناءً على سلوكياتهم السابقة على الإنترنت.

٦. استخدام التكنولوجيا لتحليل الصور والفيديوهات للتعرف على الوجوه بدون موافقة الأفراد. (الباحث)

١٧.١٣ برامج التعرف على الوجوه والذكاء الاصطناعي في الإعلام الرقمي :

انتشار تقنيات التزييف العميق (Deepfake) في الكثير من الهواتف والكومبيوترات المحمولة حيث تعمل بتحليل الوجه البشري في الصور، ومن ثم تحويلها إلى بيانات رقمية وفقا لمزايا موجودة في كل وجه (مثل المسافة بين العينين، وشكل محيط الشفاه، وتباعد الأذنين وعرض الذقن، وطول الأنف، وغيرها من المواصفات والملامح)، ويطابق الوجه مع الصور المخزنة رقمياً، في قاعدة البيانات

للوجوه، وتشترك باستخدامها لتقنيات الذكاء الصناعي والتعلم العميق ويعتبر انتهاكًا للخصوصية إن أسيئ استخدامها، وتستخدم للأغراض التالية:

١. يمكن استخدام برامج التعرف على الوجوه في أنظمة الأمان، على سبيل المثال الدخول إلى المباني والتطبيقات الأمنية العسكرية وتطبيقات الهاتف المحمول بدلاً من الأكواد السرية.

٢. يمكن استخدام برامج التعرف على الوجوه لتحسين توجيه الإعلانات والعروض التسويقية بشكل دقيق بناءً على السمات الجغرافية أو العمرية أو التعابير الوجهية.

٣. يمكن استخدام برامج التعرف على الوجوه في أمن الإنترنت لمنع الاحتيال أو الوصول غير المصرح.

٤. يمكن استخدام برامج التعرف على الوجوه في المراقبة العامة وتنفيذ القانون والتعرف على الأشخاص المطلوبين أو المشتبهين بشكل أسرع وأكثر دقة.

٥. يمكن استخدام برامج التعرف على الوجوه لتحليل العواطف والأحاسيس والانطباعات البشرية من خلال التعرف على التعابير الوجهية. (خلدون،٢٠٢٠م).

١٨.١٣ برامج التتبع في الإعلام الرقمي :

برامج التتبع في الإعلام الرقمي لتتبع سلوك المستخدمين عبر الإنترنت وجمع البيانات حولهم، وتستخدم في التسويق وتحليل البيانات وتحسين تجربة المستخدم، وهي أيضاً مصدر للدخل لمنصات التواصل الاجتماعي ومحركات البحث.

١. تستخدم برامج تحليل البيانات لتتبع سلوك الزائرين عبر المواقع الإلكترونية وتجميع البيانات حول صفحات الزيارة، والأنشطة الداخلية للصفحة، والإعلانات المتفاعلة معها.

٢. تستخدم أدوات إدارة العلاقات مع العملاء لتتبع تفاعلات العملاء عبر مواقع التواصل الاجتماعي والتطبيقات بجمع المعلومات حول تاريخ الزيارة والمشتريات والاهتمامات.

٣. تساعد أدوات تحليل التفاعلات الاجتماعية في تتبع الأنشطة والتفاعلات عبر وسائل التواصل الاجتماعي كحصر الإجابات والتعليقات والمشاركات، وتحليل هذه البيانات لفهم تأثيرها على الجمهور.

٤. تستخدم أدوات تحليل بيانات العملاء لفهم احتياجاتهم وسلوكهم وتقديم خدمات مخصصة لهم.

٥. تستخدم برامج إعلانات الإنترنت لتتبع النقرات والتفاعلات على الإعلانات الرقمية.

٦. تستخدم أدوات تحليل البريد الإلكتروني لتتبع فتح وقراءة البريد الإلكتروني، والتفاعل مع الروابط وتقديم تقارير حول أداء البريد الإلكتروني. (مبروك،٢٠٢٤).

١٩.١٣ الحملات الفيروسية في التسويق الإعلامي :

إستراتيجيات تهدف إلى انتشار المحتوى بشكل سريع عبر الإنترنت، مشابهة لانتشار الفيروسات، تستند الفكرة الأساسية على تسويق الدعاية والإعلان من منشورات أو مقطع فيديو التي تتشارك بين المستخدمين أنفسهم، حيث مشاركة المحتوى بشكل طبيعي دون تدخل مباشر من المعلن، وقد يعتبر هذا الأسلوب انتهاكاً للخصوصية.

١. محتوى جذاب: يجب أن يكون المحتوى جذاباً لإثارة اهتمام الجمهور المستهدف.

٢. سهولة المشاركة: يجب أن يكون الأسلوب سهلاً في مشاركة المحتوى عبر الوسائل الرقمية.

٣. قيمة المحتوى: يجب أن يكون المحتوى ذو قيمة مرغوبة، من ترفيه أو تعليم أو مفيداً بشكل ما.

٤. الميمات والهجمات الإعلانية: حيث تشمل استخدام الميمات والصور الفكاهية أو الهجوم الإعلاني جذب وتشجيع المشاركة.

٥. استهداف الجماهير المؤثرة: إن استهداف الشخصيات المؤثرة والمشهورة في الإنترنت يساعد في زيادة انتشار المحتوى.

٦. قدرة الانتشار السريع: يجب أن يكون المحتوى سهل الفهم بمخاطبة جميع المستويات والعقول، وسريع الانتشار.

٧. تفاعل المستخدمين: يجب أن يكون المحتوى مشجعاً على التفاعل معه بأسلوب سهل كالتعليقات والمشاركات والإعجابات.

(مركز القرار للدراسات الإعلامية،٢٠٢٢م).

٢٠١٣ التطور في تكنولوجيا المعلومات تتطور باتجاهين متعاكسين :

١. التقدم التكنولوجي يتمثل هذا الاتجاه في تقديم تحسينات وتطويرات مستمرة في التكنولوجيا المعلوماتية، من تطوير التطبيقات والبرمجيات، وزيادة سرعة المعالجات، وزيادة سعة التخزين التي تعزز كفاءة وفعالية استخدام التكنولوجيا.

٢. وبالمقابل، مع التقدم التكنولوجي تزداد التحديات والتهديدات الأمنية، حيث يتطور القراصنة الإلكترونيين والمهاجمون لاستغلال الثغرات الأمنية في التطبيقات والأنظمة الرقمية.

هذان الاتجاهان يتطوران بشكل متوازن ومتبادل، حيث يحتاج التقدم التكنولوجي إلى تعزيز الأمان والحماية للتعامل مع التحديات المتزايدة، فيلزم التصدي

للتهديدات الأمنية المتطورة في مجال الأمن السيبراني بتقديم حلول تكنولوجية متطورة ومبتكرة أيضاً.

(الباحث)

٢١.١٣ كيفية حماية خصوصيتك على الشبكة العنكبوتية؟

إذا كنت تبحث في الشبكة العنكبوتية عن معلومات، أو ترسل بريداً إلكترونياً، أو تستخدم تطبيق (GPS) في هاتفك، فأنت تتبادل البيانات في الإنترنت، ويترك أثراً خلفه من البيانات مهما كان، وتحتاج إلى حماية البيانات أثناء انتقالها، فكيف ذلك:

١. تجنب تخزين الملفات الشخصية وكلمات المرور في الهاتف المحمول أو أجهزة العمل.

٢. التأمين بكلمة مرور قوية يصعب تخمينها ومختلفة لكل حساب على الإنترنت.

٣. تغيير اسم المستخدم الخاص بالشبكة المنزلية وتغييرها كل فتره زمنية إن أمكن.

٤. تشكّل الشبكات Wi-Fi العامة المجانية في المقاهي والفنادق والأماكن العامة خطرًا أمنيًا كبيرًا، فيسهل استهدافك بواسطة المخترق.

٥. يجب عدم استخدام الشبكات Wi-Fi العامة لإنجاز المعاملات المصرفية، أفترض دوماً أنك تحت المراقبة.

٦. حافظ على برامج الحماية والتطبيقات محدثة بانتظام لسد الثغرات الأمنية.

٧. تأكد من قراءة البنود والشروط وسياسة الخصوصية، قبل الموافقة على استخدام تطبيق أو خدمة جديدة.

٨. تجنب مشاركة معلومات شخصية حساسة عبر الإنترنت، وكن حذراً مما تشاركه في مواقع التواصل الاجتماعي.

٩. التحكم بضبط إعدادات الخصوصية على منصات التواصل الاجتماعي لمشاركة المعلومات مع الأشخاص الموثوق بهم.

١٠. لا تنس تسجيل الخروج من حساباتك بشكل صحيح عندما لا تستخدمها، فمجرد إغلاق علامة التبويب أو المستعرض ليس كافيًا. (كاسبر سكاي،)

٢٢.١٣ كيفية الحماية من الهجمات السيبرانية؟

لحماية الأنظمة من الهجمات السيبرانية، يجب إتباع بعض الإجراءات الأمنية ومنها:

١. يجب التأكد من تثبيت برامج الحماية المضادة للفيروسات والبرامج الضارة وتحديثها بانتظام.

٢. يجب تفعيل جدار الحماية على الأجهزة لمنع وصول الهجمات من الخارج.

٣. حافظ دوماً بإنشاء نسخ احتياطية من البيانات الهامة.

٤. داوم على تحديث الأنظمة والبرامج الموثوقة لسد الثغرات الأمنية.

٥. احذر عند فتح مرفقات البريد الإلكتروني من مصادر غير معروفة، وتحقق من هوية المرسل.

٦. تحقق من روابط البريد الإلكتروني ولا تقم بإدخال معلومات شخصية عبر روابط مشبوهة فقد تكون احتياليه.

٧. استخدم كلمات مرور قوية ولا تشاركها مع الآخرين.

٨. قم بتدريب موظفيك وأفراد عائلتك على أخطار الأمن السيبراني وكيفية التعامل معها.

(الشامسي،٢٠٢٣).

٢٣.١٣ كيفية تجنب المكالمات والتصيد الاحتيالي؟

لتجنب المكالمات والتصيد الاحتيالي (Phishing Calls)، إليك الإجراءات الوقائية:

١. عدم الرد على مكالمات المجهولة.

٢. عدم الضغط على روابط مجهولة.

٣. عدم تقديم المعلومات الشخصية والمالية عبر المكالمات الهاتفية.

٤. التحقق من هوية المتصل، عن طريق الاتصال بالشركة مباشرة.

٥. تنبيه الجهات المختصة والإبلاغ عن المكالمات المشبوهة للجهات الأمنية المعنية. (الباحث)

٢٤.١٣ كيف تتأكد من صحة وموثوقية المعلومات في الإعلام الرقمي :

الذي يعتبر أمرًا حيويًا لاتخاذ القرارات المسؤولة.

١. التحقق من مصدر المعلومات ومصداقية الموقع الإلكتروني قبل اعتمادها ومشاركتها عبر وسائل التواصل الاجتماعي.

٢. التحقق من التوقيت الزمني للمعلومات، والا تكون قديمة أو غير دقيقة.

٣. تقييم ومقارنة النشرات والتقارير والتحقق من مصداقية الناشرين ومصادر معلوماتهم.

٤. استخدام الأدوات التحليلية البيانية والتقنيات المتقدمة للتحقق من صحة البيانات ومصداقيتها. (الباحث)

٢٥.١٣ كيفية التدريب والتوعية ضد الانتهاكات في الإعلام الرقمي :

تدريب وتوعية الأفراد ضد الانتهاكات في الإعلام الرقمي والحفاظ على الأمان والخصوصية عبر الشبكة العنكبوتية، ولتحقيق هذا الهدف:

١. توفير الدورات التدريبية وورش العمل حول أخطار الانتهاكات في الإعلام الرقمي وكيفية التعامل معها، ومن الموضوعات والعناوين المقترحة " الوقاية من الاحتيال الإلكتروني، والتحقق من صحة المعلومات، وكيفية الحماية من البرمجيات الخبيثة، والوعي بحفظ الخصوصية".

٢. التثقيف السلوكي الآمن عبر الإنترنت: ومن أمثلة الموضوعات عدم فتح روابط مجهولة، وعدم مشاركة المعلومات الشخصية، ومراجعة إعدادات الخصوصية على المنصات، واستخدام كلمات مرور قوية.

٣. تشجيع المشاركة المسؤولة: ونقصد به عدم نشر المعلومات الكاذبة أو غير المدققة، والتحقق من مصادر المعلومات قبل مشاركتها، وإنشاء بيئة رقمية إعلامية آمنة.

٤. تطوير المهارات الرقمية والتدريب على مهارات البحث والتحليل النقدي وإدارة الخصوصية والحماية من الاحتيال والاختراقات الإلكترونية.

٥. توفير الموارد الإرشادية والمعلومات الخاصة بأمان الإنترنت والخصوصية الرقمية عبر المواقع والمنصات التعليمية ومن خلال الجهات الحكومية المختصة.

٦. تعزيز الثقافة الرقمية في المجتمعات من خلال الحوار والمناقشة حول أخطار الإرهاب السيبراني وضمان استخدام آمن ومسؤول للتكنولوجيا. (الباحث)

٢٦.١٣ رأي الباحث في التقنية الإلكترونية والبرامج المتطورة :

تتفاوت آراء العلماء في التقنية الإلكترونية بناءً على مجال تخصصهم وتجاربهم الشخصية والعلمية، فيرى الباحث أن التقدم التقني الإلكتروني والبرامج المتطورة أحدث ثورةً في العديد من المجالات العلمية فهو يسهل العمليات الحيوية ويوفر فرصًا جديدة للتطوير والابتكار، كما أن التحديات والمخاطر التي تصاحب التقنية الإلكترونية المتقدمة بالرغم من فوائدها، وبوجود انتهاك الخصوصية، والهجمات السيبرانية، وتأثيرات التحول الرقمي، ننوه بأهمية برامج الحماية في مواجهة التهديدات الأمنية، فضلاً عن الاستثمار في البحث والتطوير المستمر في مجال الأمن الرقمي وتطوير برامج الحماية، ومهما تطورت برامج الحماية فالهجمات السيبرانية تتطور أيضاً وتتطلب استجابات سريعة لصدها. **(الباحث)**

٢٧.١٣ منذ دخولك في الانترنت فانت مراقب عملياً :

"منذ دخولك في الإنترنت فأنت مراقب عملياً" هذه الفكرة العامة توضح أن استخدام الإنترنت قد يعرضك للمراقبة أو التتبع من قبل الجهات سواء كانت شركات التكنولوجيا أو المتسللين الإلكترونيين أو الحكومات.

١. تستخدم الشركات التكنولوجية والمواقع الإلكترونية والتطبيقات التواصلية تقنيات لتتبع نشاط المستخدمين على الإنترنت، مثل ملفات تعريف الارتباط (Cookies)، وتحليلات الويب (Web analytics)، وعلامات التتبع (Tracking tags)، حيث يحلل سلوك الزائرين.

٢. تستخدم الحكومات والمؤسسات الأمنية، والمتسللين الإلكترونيين استخدام تقنيات متقدمة لمراقبة الأنشطة ومراقبة الاتصالات وتحليل البيانات والتجسس على المكالمات الشخصية.

ومن هذا المنطلق نبين أهمية حماية الخصوصية والأمان الرقمي بحماية البيانات الشخصية على الإنترنت. (الباحث)

* الإطار المنهجي *

١٥- نوع ومنهج الدراسة :

تتضمن المنهج ونظريات الدراسة:

١.١٥ المنهج الوصفي :

تهدف إلى فهم ووصف واستكشاف الظواهر، وتركز على فهم العمق والتعقيد للتجارب الشخصية وتسليط الضوء على الجوانب النفسية والعاطفية والاجتماعية للتحقق من الأحداث والظواهر والتفاصيل والعلاقات التي تحدث في الواقع، كما يضم استبانة الرأي، من خلال الدراسة الميدانية بالعينة ولمعرفة خصائص ورأي ومشاعر وميول واتجاهات افراد (عينة البحث) وإدراكهم بخطورة الهجمات السيبرانية في الشبكة العنكبوتية وطريقة تعاملهم مع تلك التهديدات وجمع البيانات الكمية وتحليلها بطرق إحصائية.

٢.١٥ نظريات الدراسة:

- **نظرية المجال العام** (Public Sphere Theory)، تشكيل رأى عام بأفكارها للمفاهيم والمناقشات قادراً على بناء وتوظيف نقاشات عقلانية منطقية متعلقة بالقضايا العامة والمشتركة وتؤثر على كافة المجتمع اعتماداً على وسائل الإعلام، (المهدي،٢٠١٨)
- **نظرية التحول الرقمي** (Digital Transition Theory): التأثيرات والتحولات التدريجية لوسائل الإعلام الناجمة عن ضغوطات خارجية لاستخدام التكنولوجيا الرقمية في مجال الإعلام. (مركز القرار للدراسات الإعلامية،٢٠٢١)

- **نظرية الثقافة الرقمية** (Digital Culture Theory): فهم التغيرات الثقافية نتيجة تأثير التكنولوجيا الرقمية على الثقافات والممارسات الاجتماعية. (حسن،٢٠٢١م)
- **نظرية الحوكمة الرقمية** (Digital Governance Theory): كيفية إدارة وتوجيه استخدام التكنولوجيا الرقمية من قبل الحكومات لتحسين خدماتها وتفاعلها مع المواطنين، (حاجة،٢٠٢٣م).
- **نظرية التطور التكنولوجي** (Technological Evolution Theory): تركز على كيفية تطور التكنولوجيا الرقمية وتأثيرها في حل المشاكل على المجتمع بأكمله، (حاجة،٢٠٢٣م).
- **نظرية الاندماج الإعلامي** (Media Convergence Theory): تغييرات واضحة تحدثها تكنولوجيا الإعلام على تفاعل الوسائط المختلفة في العصر الرقمي وفي طبيعة التواصل البشري،

(مركز القرار للدراسات الإعلامية،٢٠٢١م)

١٦- أدوات جمع البيانات وخطة الدراسة :

- صحيفة الاستبانة وأداة البحث تستخدم لجمع البيانات الكمية من مجموعة واسعة من المشاركين عن طريق أسئلة محددة.
- تحديد الأفراد المستهدفين للدراسة والذين سيشاركون بتقديم البيانات وتعبئة الاستبانة من المهتمين في مجال الدراسة بتقنية المعلومات.
- جمع البيانات الأولية والأساسية أو المباشرة من مفردات مجتمع البحث، عن طريق الاستبانة، في مجال الاعلام الرقمي والتقنية الحاسوبية.
- تحليل البيانات المجمعة وفهم النتائج والاستنتاجات.

- عرض النتائج والاستنتاجات يوضح المعلومات المكتسبة والتحليلات المستخدمة.
- تحرير توصيات الدراسة.

١٧- فهم صحيفة الاستبانة وتقسيم الدراسة :

- تهدف الأسئلة البحثية لأخذ أراء المختصين في التكنولوجيا الرقمية، والجمهور المهتمين بوسائل الإعلام الرقمي بوضعهم البيانات والمعلومات الشخصية على هواتفهم و مواقع وسائل التواصل الاجتماعي، والتخزين السحابي التي تجعل بياناتهم ومعلوماتهم عرضة للانتهاكات والسرقة، وما مدى قدرتهم على حماية بياناتهم باستخدام البرامج المضادة من التطفل، وقدرة الشركات المشغلة للمواقع في المحافظة على بياناتهم، وقدرة الهيئات الحكومية على حمايتهم من الإرهاب السيبراني. وما مدى ثقة المختصين والجمهور في المعلومات الوثائقية والفيديوهات والأخبار المرئية في ظل تطور الأعلام الرقمي والذكاء الاصطناعي.
- تم تصميم صحيفة الاستبانة لجمع البيانات وتشمل مجموعة من الأسئلة المغلقة، ومنها:

١.١٧ الأسئلة الديموغرافية:

١. العمر: لتحديد أعمار المتأثرون في وسائل التواصل الاجتماعي. (أصغر من ١٨ سنة – بين ١٨ و٣٠ سنة – أكبر من ٣٠ سنة)

٢. الجنس: لتحديد الفئة الأعلى تأثراً من الجنسين (ذكر – أنثى)

٣. المؤهل العلمي: لمعرفة مدى ثقافة المتأثرون بالدراسة. (ثانوي فأقل – جامعي – دراسات عليا)

٤. موقع العمل: لمعرفة علاقة العينة بالدراسة (مدارس حكومية أو أهلية – شركة بترولية – شركة اتصالات – هيئات حكومية وأهلية – مؤسسات طبية)

٥. الوظيفة: لمعرفة نوع عمل العينة ومدى معرفته بالإعلام الرقمي (طالب مدرسي – موظف مجال الحاسب الألى والمعلومات– موظف مجال الموارد البشرية – موظف المجال البنكي والمالي – مجالات أخرى)

- تم صياغة بعض الأسئلة التخصصية البحثية لمعرفة مدى العلاقة بين البيانات الديموغرافية وارتباطها في ساحات وسائل التواصل الاجتماعي والإنترنت، وفهم وجهات النظر للمستفيدين، وتم تقسيم الدراسة لتغطية الجوانب الآتية: محور انتهاكات الخصوصية ومحور الهجمات السيبراني ومحور فقدان الثقة في الإعلام الرقمي، وذلك باستخدام مقياس ليكارث الخماسي للإجابة على الاستبيان.

٢.١٧ محور انتهاكات الخصوصية:

ونعني بتبادل المعلومات شخصية، التي قد تحدث نتيجة سرقة وانتهاكات قوانين حماية البيانات والتأثير السلبي على الأمان الرقمي للأفراد والمؤسسات.

٦. هل تعتقد أنه يجب على مستخدم صفحات الإنترنت أن يكون على دراية وإدراك لكيفية حماية بياناته؟ (لمعرفة مدى إدراك المستخدم وقدرته واطلاعه على حماية البيانات).

٧. هل تعتقد أن الشركات والمؤسسات التي تجمع بياناتك الشخصية مسؤولة في حمايتها؟، (لمعرفة رأي المستخدم ما إذا كانت المسؤولية تقع على عاتق الشركات والمؤسسات بحماية بيانات عملائها).

٨. هل تعتقد أن هناك حاجة لمزيد من التوعية حول حقوق الخصوصية وأمان البيانات الشخصية؟، (لمعرفة رغبة المستخدم بزيادة وسائل التوعية في مجال الخصوصية وحماية البيانات، وأهمية حماية الخصوصية الرقمية وتقليل المخاطر التكنولوجية في الإعلام الرقمي).

٩. هل تعتقد أن تحقيق الخصوصية في البيئة الرقمية حقاً أساسياً للأفراد في ظل التقدم التكنولوجي؟، (لمعرفة رأي المستخدم بحقوقيات وحفظ بياناته)

١٠.هل تعتقد أن الهجمات السيبرانية تشكل تهديداً خطيراً على المستوى العالمي؟، (لمعرفة رأي المستخدم بالهجمات السيبرانية).

١١.هل تعتقد أنه لا بد من التحقق من مصادر المعلومات قبل مشاركتها أو الاعتماد عليها؟، (لمعرفة رأي العينة بأنه يتحقق من المعلومات قبل تداوله).

١٢. هل تعتقد أن هناك حاجة إلى توعية أكبر حول كيفية التعامل مع المعلومات الرقمية والتحقق من صحتها؟، (لمعرفة استكشاف أهمية التوعية بأمان المعلومات وسبل تعزيز الوعي الرقمي لدى الجمهور والعاملين وحاجتهم الى كيفية التعامل مع المعلومات الرقمية).

١٣. هل تعتبر التقنيات الجديدة مثل التعرف على الوجوه والتتبع الرقمي انتهاكًا للخصوصية؟ ، (لمعرفة ما إذا بعض التقنيات الحديثة تشكل انتهاكا للخصوصية).

٣.١٧ محور الهجمات السيبرانية:

تقوم جماعات إرهابية أو أفراد بالهجمات والاختراقات السيبرانية، وبث البرمجيات الخبيثة، والتلاعب بالبيانات والمعلومات، والتأثير السلبي على البنية التحتية للدول والمؤسسات، ويكون التأثير على الاقتصاد والأمن القومي، والفوضى في الانظمة.

١٤.هل توافق أن تقنيات الوقاية والدفاع من قبل الجهات المعنية ضد الهجمات السيبرانية كافية؟، (لمعرفة رأي المستخدم ما إذا كانت التقنيات ووسيلة الدفاع من قبل الشركات والجهات المعنية ضد الهجمات السيبرانية كافية، بتحليل دور الأمن السيبراني والتقنيات الحديثة في حماية البيانات).

١٥.هل تعتبر تشديد العقوبات على المهاجمين السيبرانيين بما يكفي لردعهم؟، (لمعرفة رأي المستخدم بأن تقييم السياسات والتشريعات الحالية المتعلقة

بحماية الخصوصية وتقديم مقترحات لتعزيزها وتحسينها وأن العقوبات للإرهاب السيبراني كافية).

١٦.هل تثق في المعلومات التي تجدها عبر الوسائط الاجتماعية والمواقع الإلكترونية؟، (لمعرفة رأي العينة في ثقته بمعلومات وسائل التواصل الاجتماعي)

١٧.هل تعتقد أن وسائل الإعلام الرقمية تنشر معلومات دقيقة وموثوقة بشكل عام؟، (لمعرفة رأي العينة بوسائل الإعلام الرقمية).

١٨.هل لديك ثقة في الصور والفيديوهات المنشورة عبر منصات التواصل الاجتماعي في ظل التطور التكنولوجي والذكاء الاصطناعي ؟، (لمعرفة رأي العينة وثقته في الصور والفيديوهات على وسائل الاعلام الرقمي التي قد تكون مفبركة).

٤.١٧ محور فقدان الثقة في الإعلام الرقمي:

تعاني وسائل الإعلام الرقمية من ظاهرة الثقة بالمعلومات والأخبار التي تنشرها وسائل التواصل الاجتماعي وتحتاج لزيادة مستوى الشفافية، والنزاهة، والصدق، فما رأي المستخدم؟

١٩. هل تعتقد أن التدريب والتوعية بشأن أخطار الإرهاب السيبراني يمكن أن يساعد في الوقاية منه؟، (لمعرفة رأي العينة بالتدريب والتوعية لمخاطر الإرهاب السيبراني تساعد على تقليل التهديدات السيبرانية وحماية البيانات بشكل فعال).

٢٠.هل تؤيد مشاركة وتعاون الحكومات والشركات والمؤسسات الخاصة استخدام تقنيات الذكاء الاصطناعي في مكافحة الإرهاب السيبراني؟، (لمعرفة رأي العينة في تضامن الجهات مشتركة لمكافحة الإرهاب السيبراني، وتعزيز

استراتيجيات تصور الشركات والمؤسسات في أمن المعلومات للحد من التهديدات السيبرانية، بقياس فعالية التدابير الأمنية المتخذة وتقييم أثرها).

٢١.هل تعتقد أن الحكومات يجب أن تكون أكثر شفافية ووضوحاً في تحليل الهجمات السيبرانية والتعامل معها؟، (لمعرفة اعتقاد العينة في موضوع الشفافية والإفصاح عن الهجمات السيبرانية).

٢٢.هل أثرت الهجمات السيبرانية على حياتك الشخصية أو عملك؟، (لمعرفة تأثير الهجمات السيبرانية على الأفراد والمؤسسات).

٢٣.هل تعتقد أن هناك انحياز في وسائل الإعلام الرقمية؟، (لمعرفة مدى الثقة في وسائل الإعلام بأخبارها)

٢٤.هل تعتقد بأن المعلومات الرقمية تتأثر بالتلاعب والتحريف؟، (لمعرفة مصداقية المعلومات)

٢٥.هل تعتقد أن هناك نقصًا في التحقق من المصادر على الإنترنت؟، (لمعرفة مصداقية المصادر)

٢٦.هل تشعر بالإحباط والإرباك عند محاولة فصل الحقيقة عن الشائعات والمعلومات المضللة على وسائل التواصل الاجتماعي؟، (التأثير على القارئ)

٢٧.هل تفضل الاعتماد على المحتوى الرقمي من قبل المؤسسات الإعلامية التقليدية بدلاً من المصادر الرقمية الجديدة؟ ، (لمعرفة النوع المفضل في الإعلام بشكل عام)

٢٨.هل تشعر بأن هناك انخفاضًا في القيم الاجتماعية والثقافية للإعلام الرقمي بسبب نقص المصداقية؟، (لمعرفة رأي المجتمع)

١٨- المقاييس والاختبارات الإحصائية :

ومن المقاييس في الاختبارات الإحصائية باستخدام برنامج احصائي (SPSS).

١.١٨ **النزعة المركزية** (Central Tendency):

- المتوسط الحسابي (Average/ mean)، واستخدام الأداة (Compute Variable:)
- التكرار (Frequency) = عدد التكرار للعينة
- النسب المئوية (Percentage) = عدد قيم العينة / مجموع القيمة الكلية للعينات x ١٠٠

٢.١٨ **التشتت** (Variation):

- المدى (Range) = اعلى قيمة – أدنى قيمة
- الانحراف المعياري (standard deviation)

٣.١٨ **الانحدار البسيط** (Simple Regression)

١٩- الأدوات المستخدمة في برنامج (SPSS)

- الأداة (Compute Variable:)، لاحتساب المعدل المتوسط الحسابي للفقرات (الاسئلة) في المحور
- الأداة (BRVARIATE) معامل بيرسون لقياس الصدق الداخلي للاستبانة.
- الأداة (RELIABILITY ANALYSIS) الفا كرونباخ Cronbach's Alpha)لاختبار ثبات الاستبانة.
- الأداة (Frequencies) لتحليل البيانات الإحصائية.
- الأداة (Linear) الانحدار الخطي البسيط

٢٠- النتائج (Results):

- عمل رسم بياني (Histogram) للنقاط الإحصائية باستخدام برنامج (SPSS) وتمثيل البيانات بشكل بصري لتسهيل فهم وتقييم توزيع البيانات، حيث يبين درجة انتشار البيانات والسلوك المركزي للبيانات.
- تم التأكد من صدق الاستبيان وتم اختباره على (١٠) عينة بحساب تحليل الصدق العاملي، والتأكد أن الفقرات تنتمي لمحاورها، وحساب نسبة الثبات من خلال برنامج (SPSS) للأسئلة الأساسية وعددها (١٦) ودل على قبولية أداة الاستقصاء ويؤكد صلاحيتها للتطبيق.

٢١- مجتمع الدراسة :

شكل مجتمع الدراسة الميدانية في المملكة العربية السعودية (من المختصين في تقنية المعلومات في الإدارات والشركات والهيئات والمهتمين بخصوصية المعلومات الشخصية)، ومن هذه الإدارات (إدارة تقنية المعلومات بميناء جدة الإسلامي، إدارة تقنية المعلومات بالخطوط السعودية، إدارة تقنية المعلومات بشركة أرامكو السعودية، وبعض من العينات العشوائية بالمجتمع في مدينة جدة.)

١.٢١ عينة الدراسة:

تم اختيار عينة المختصين عدد (٣٠) مبحوثاً، ومن العينات العشوائية عدد (٣٩) عينة، بناءً على الذين يمتلكون معلومات أو تجارب ذات علاقة. فالهدف هو اكتساب فهم أعمق لتجارب ومشاعر الأفراد وفهم جوانبهم الشخصية، وتم جمع البيانات عن طريق الاستبيانات.

٢.٢١ حدود الدراسة:

١. **الحدود الجغرافية ومجتمع البحث:** يتم جمعها بطريقة عشوائية على كافة شـــرائح المجتمع.

٢. **الحدود البشرية، العمر والجنس:** من الذكور والإناث وعلى جميع المستويات التي تمثل شرائح المجتمع من مواطنين ومقيمين، وذلك للحصول على بيانات لا تمثـــل فئة معينة او عرق معين.

٣. **الحدود الزمنية والوقت:** اقتصرت الدراسة في الفترة الزمنية علـــى العـــام ٢٠٢٤ الميلادي في الشهر الثالث (مارس).

٤. **الحدود الكمية:** وقد كانت أعداد العينة بما يقارب (٦٩) عينة مفردة.

٢٢- قياس متغيرات ومحاور الدراسة

١.٢٢ صدق الاتساق الداخلي

للتحقق من صدق الاتساق الداخلي ومصداقية محتوى قائمة الاستقصـــاء تـــم تقييم درجة التناسق ومدى قدرة المقياس على قياس ما يفترض قياسه، وتشير البيانـــات الى قوة العناصر بمحاورها بصفة عامة وأنها سوف تحقق المقياس.

٢.٢٢ تقييم ثبات المحاور

يستخدم الاختبار بمعامل الفاكرونباخ لمعرفة إمكانية الاعتمـــاد علـــى قائمـــة الاستقصاء في قياس بيانات تتسم بالثبات وتم تطبيقه على عينة مكونـــة مـــن (٦٩) عينة وجاءت النتائج كما يلي:

تم حساب نسبة الثبات من خلال برنامج (SPSS) لمحاور الأســـئلة الأساســـية وعددها (٢٣)، فجاءت محور انتهاكات الخصوصية بعدد (٨) أسئلة فكانـــت معامـــل

ألفا كرون باخ بنسبة (٠.٨٦٢) وعند حذف السؤال (٩) وعدم اعتباره في الاستبيان يرتفع الفاكرون باخ إلى (٠.٨٧٥)، ومحور الإرهاب السيبراني بعدد (٥) أسئلة فجاءت معامل الفاكرونباخ بنسبة (٠.٥٣٦) وعند حذف السؤال (١٥) وعدم اعتباره في الاستبيان يرتفع نسبة الفاكرونباخ إلى (٠.٦١٥)، أما محور فقدان الثقة في الإعلام الرقمي بعدد (١٠) أسئلة فجاءت معامل ألفاكرونباخ بنسبة (٠.٦٧٨) وعند حذف السؤال (٢٢) وعدم اعتباره في الاستبيان يرتفع نسبة الفاكرونباخ إلى (٠.٧٧٢)، مما يدل على قبولية أداة الاستقصاء ويؤكد صلاحيتها للتطبيق.

٢٣- نتائج البيانات الإحصائية :

- تشير البيانات الديموغرافية الى استجابات المبحوثين أكثرهم من الأعمار بين ١٨ و٣٠ سنة بنسبة (٥٥.١%) وهم من الإناث بنسبة (٥٦.٥%)، وغالبية المبحوثين ذو المؤهلات الجامعية بنسبة (٦٢.٣%)، والنسبة الأعلى في المدارس الحكومية والأهلية بنسبة (٥٢.٢%)، وأما الوظائف التي سوف نركز عليها هم موظفي في مجال الحاسب الآلي وتقنية المعلومات بنسبة (٤٣.٥%) وهم الذين لديهم خبرة في مجال الخصوصية والهجمات السيبرانية.

- تشير البيانات في محور انتهاكات الخصوصية الى استجابات المبحوثين حول العبارات بالإجابة على السؤال (٦) فعبارتي أوافق بشدة بعدد (٥٢) ونسبة (٧٥.٤%) ، وأوافق بعدد (١١) ونسبة (١٥.٩%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (٧) فعبارتي أوافق بشدة بعدد (٤٧) ونسبة (٦٨.١%) ، وأوافق بعدد (١٣) ونسبة (١٨.٨%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (٨) فعبارتي أوافق بشدة بعدد (٥٣) ونسبة (٧٦.٨%) ، وأوافق بعدد (١٠) ونسبة (١٤.٥%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا

السؤال، أما بالنسبة للسؤال (٩) فعبارتي أوافق بشدة بعدد (٤٢) ونسبة (٦٠.٩%) ، وأوافق بعدد (٢٢) ونسبة (٣١.٩%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (١٠) فعبارتي أوافق بشدة بعدد (٤٩) ونسبة (٧١.٠%) ، وأوافق بعدد (١٤) ونسبة (٢٠.٣%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (١١) فعبارتي أوافق بشدة بعدد (٥٢) ونسبة (٧٥.٤%) ، وأوافق بعدد (١١) ونسبة (١٥.٩%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (١٢) فعبارتي أوافق بشدة بعدد (٤٩) ونسبة (٧١.٠%) ، وأوافق بعدد (١٧) ونسبة (٢٤.٦%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، أما بالنسبة للسؤال (١٣) فعبارتي أوافق بشدة بعدد (١٩) ونسبة (٢٧.٥%) ، وأوافق بعدد (٢٢) ونسبة (٣١.٩%)، أي أن مجموعة النسبتين الأكثر بالموافقة للعبارة في هذا السؤال، فيبين أن محور انتهاكات الخصوصية في سياق الموضوع تحتاج الى توعية أكبر وأن المستخدم يجب ان يكون على دراية بكيفية حماية بياناته وأن الشركات مسؤولة عن تلك البيانات المسجلة لديهم وان تداولها بغير حق يعتبر انتهاكاً للخصوصية حيث ينظر المستخدمون إلى الخصوصية كأصل شخصي وهذا ما يتفق مع دراسة (Fang،٢٠٢٣)، وأيضا تتفق مع دراسة (إبراهيم،٢٠٢١م) حيث أن الخصوصية حق من حقوق الإنسان، كما أن وجه الاتفاقية بدراسة (كدواني،٢٠٢٠م) أن إعدادات الخصوصية لا تحمي المستخدم ولا تمنع بياناته عن مالكي الخدمة ويفترض على الشركات والمواقع تعمل على حماية خصوصية المستخدم وليس تداوله بأسلوب تجاري، كما أكده دراسة (محمدين،٢٠٢٢م) بأن سياسية حماية الخصوصية بها بعض الملاحظات والتضارب، فيجب قراءة سياسيات الخصوصية بتمعن.

- تشير البيانات محور الهجمات (الإرهاب) السيبرانية الى استجابات المبحوثين حول العبارات بالإجابة على السؤال (١٤) فعبارات محايد بعدد (82) ونسبة (40.6%)، وأوافق بعدد (١٦) ونسبة (٢٣.٢%)، ولا أوافق بعدد (١٤) ونسبة (٢٠.٣%) أي أن الترجيح بأن تقنيات الدفاع ليست كافية لحماية المستخدمين وهذا ما يؤكده مضمون الإجابات، أما بالنسبة للسؤال (١٥) فعبارتي أوافق بشدة بعدد (٢٢) ونسبة (٣١.٩%)، و أوافق بعدد (١٨) ونسبة (٢٦.١%) ذات النسبة الأغلبية بالموافقة على تشديد العقوبات، أما بالنسبة للسؤال (١٦) فعبارتي لا أوافق بعدد (٢٨) ونسبة (٤٠.٦%)، و لا أوافق بشدة بعدد (١٧) ونسبة (٢٤.٦%) تبين المجموعتين بعم الثقة في الإعلام الرقمي للأغلبية، أما بالنسبة للسؤال (١٧) فعبارتي لا أوافق بعدد (٣٠) ونسبة (٤٣.٥%)، ولا أوافق بشدة بعدد (١٣) ونسبة (١٨.٨%) هما النسبتين التين تؤكدان فقدان الثقة في الإعلام الرقمي، أما بالنسبة للسؤال (١٨) فعبارتي لا أوافق بعدد (٣٤) ونسبة (٤٩.٣%)، ولا أوافق بشدة بعدد (١٣) ونسبة (١٨.٨%) تؤكدان ما سبق وأن الهجمات السيبرانية لها أبعاد لمخاطر الإعلام الرقمي ووسائل التواصل الاجتماعي تأكيدا لدراسة (فخرالدين،٢٠٢٣)، وأنه لا بد من وضع استراتيجية موحدة للأمن الإلكتروني، وزيادة العقوبات حول جرائم الأمن السيبراني، كما جاء في رأي الأغلبية التي أتت متوافقة مع دراسة (قرني، خطاب،٢٠٢٢م).
- تشير البيانات في محور فقدان الثقة في الإعلام الرقمي الى استجابات المبحوثين حول العبارات بالإجابة على السؤال (١٩) فعبارتي أوافق بشدة بعدد (٣٧) ونسبة (٤٤.٩%)، وأوافق بعدد (٢٣) ونسبة (٣٣.٣%)، أي الترجيح أن التدريب والتوعية بشأن مخاطر الإرهاب السيبراني يمكن أن يساعد في الوقاية منه وهذا ما يؤكده مضمون الإجابات، أما بالنسبة للسؤال (٢٠) فعبارتي أوافق بشدة بعدد (٣١) ونسبة (٥٣.٦%)، وأوافق بعدد (٢١) ونسبة (٣٠.٤%)، من مؤيدي

مشاركة وتعاون الحكومات والشركات والمؤسسات الخاصة استخدام تقنيات الذكاء الاصطناعي في مكافحة الإرهاب السيبراني، أما بالنسبة للسؤال (٢١) فعبارتي أوافق بشدة بعدد (٢٦) ونسبة (٣٧.٧%)، وأوافق بعدد (١٨) ونسبة (٢٦.١%) توضحان بأن الحكومات يجب أن تكون أكثر شفافية ووضوحاً، أما بالنسبة للسؤال (٢٢) فجاءت نتائجها عكسية وتم حذفها من المعادلة، أما بالنسبة للسؤال (٢٣) فعبارتي أوافق بعدد (٣٠) ونسبة (٤٣.٥%)، و أوافق بشدة بعدد (١٦) ونسبة (٢٣.٢%) بأن هناك انحياز في وسائل الإعلام الرقمية، أما بالنسبة للسؤال (٢٤) فعبارتي أوافق بعدد (٣١) ونسبة (٤٤.٩%)، وأوافق بشدة بعدد (٢٩) ونسبة (٤٢.٠%) بأن المعلومات الرقمية تتأثر بالتلاعب والتحريف، أما بالنسبة للسؤال (٢٥) فعبارتي أوافق بعدد (٣٢) ونسبة (٤٦.٤%)، وأوافق بشدة بعدد (٢٠) ونسبة (٢٩.٠%) أن هناك نقصًا في التحقق من المصادر على الإنترنت، أما بالنسبة للسؤال (٢٦) فعبارتي أوافق بعدد (٣١) ونسبة (٤٤.٩%)، وأوافق بشدة بعدد (١٦) ونسبة (٢٣.٢%) يبين مدى الشعور بالإحباط والإرباك بشأن الشائعات والمعلومات المضللة على وسائل التواصل الاجتماعي، أما بالنسبة للسؤال (٢٧) فعبارتي محايد بعدد (٣١) ونسبة (٤٤.٩%)، وأوافق بعدد (١٧) ونسبة (٢٤.٥%) يبين تفضيل الاعتماد على المحتوى الرقمي من قبل المؤسسات الإعلامية التقليدية بدلاً من المصادر الرقمية الجديدة، أما بالنسبة للسؤال (٢٨) فعبارتي محايد بعدد (٢٧) ونسبة (٣٩.١%)، وأوافق بشدة بعدد (٢٦) ونسبة (٣٧.٧%) يبين رأي العينات بأن هناك انخفاضًا في القيم الاجتماعية والثقافية للإعلام الرقمي بسبب نقص المصداقية، وبناءً على المعطيات فالتأثر بفقدان الثقة في الإعلام الرقمي بتصاعد مستمر وهذا ما أكدة دراسة (الغيطي،٢٠٢١) في دراسته للنخب المتخصصين في مجال تقنية المعلومات بأن اعتماد الجمهور على المواقع التفاعلية ووسائل التواصل الاجتماعي وانتشار الشائعات والأخبار المضللة تفقد الثقة بالتكنولوجيا الإعلامية.

٢٤- تحليل فرضيات الدراسة :

١. يوجد تأثير ذو علاقة ارتباطية معنوية ذات دلالة إحصائية بين انتهاك الخصوصية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي.

٢. يوجد تأثير ذو علاقة ارتباطية معنوية ذات دلالة إحصائية بين الهجمات السيبرانية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي.

النتيجة النهائية

معاملات الانحدار الخطي البسيط									
المتغير المستقل	المتغير التابع	R	R2	F	F-sig	B	t	t - sig	VIF
انتهاك الخصوصية	فقدان الثقة	٠.٥٥٤	٠.٣٠٧	٢٩.٦٩٤	٠.٠٠٠	٠.٤٧٨	٥.٤٤٩	٠.٠٠٠	١.٠٠٠
الهجمات السيبرانية		-٠.٠٠٧	٠.٠٠٠	٠.٠٠٣	٠.٩٥٧	-٠.٠٠٥	-٠.٠٥٤	٠.٩٥٧	١.٠٠٠

من أجل معرفة العلاقة بين المتغيرات ، تم استخدام الانحدار الخطي البسيط لكل فرضية وأظهرت النتائج في الفرضية الأولى بأنه يوجد تأثير ذو علاقة ارتباطية معنوية ذات دلالة إحصائية بين انتهاك الخصوصية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي، وأن الانحدار معنوي من خلال قيمة (F) البالغ (٢٩.٦٩٤) بدلالة (Sig) البالغ قيمته (٠.٠٠٠) أصغر من مستوى المعنوية (٠.٠١) وتفسر النتائج أن المتغيرات تفسر (٢٩%) من التباين الحاصل في محور فقدان الثقة في الإعلام الرقمي ونرفض الفرض الصفري ونقبل الفرض البديل، وذلك بالنظر إلى معامل التحديد (R2) البالغ (٠.٣٠٧)، كما جاءت بيتا (B) التي توضح العلاقة بقيمة (٠.٤٧٨)

ذات دلالة إحصائية حيث يمكن استنتاج ذلك من قيمة (t) البالغ (٥.٤٤٩)، والدلالة المرتبطة بها (t-sig) بقيمة (٠.٠٠٠)، وأن فقدان الثقة عملية طردية بانتهاك الخصوصية بوحدة (٠.٥٥٤) وحده. وقيمة معاملات التضخم (VIF) Variance Inflation Factors ويساوي (١.٠٠٠)، ومعاملات التسامح (Tolerance) ويساوي (١.٠٠٠)، وبالمعادلة حيث VIF = 1 / Tolerance، والتي يتبين منها عدم وجود مشكلة بين المتغيرات حيث كانت معاملات التضخم اقل من (٣).

وفي الفرضية الثانية بأنه لا يوجد تأثير ذات دلالة إحصائية بين الهجمات السيبرانية في مجال الإعلام الرقمي وفقدان الثقة في الأنظمة الرقمية والإعلام الرقمي، وأن الانحدار غير معنوي من خلال قيمة (F) البالغ (٠.٠٠٣) بدلالة (Sig) البالغ قيمته (٠.٩٥٧) أكبر من مستوى المعنوية (٠.٠٥) وتفسر النتائج أن نقبل الفرض الصفري في محور فقدان الثقة في الإعلام الرقمي، وذلك بالنظر إلى معامل التحديد (R2) البالغ (٠.٠٠٠)، كما جاءت بيتا (B) التي توضح العلاقة بقيمة (٠.٠٠٥) ذات دلالة إحصائية حيث يمكن استنتاج ذلك من قيمة (t) البالغ (٠.٠٥٤-)، والدلالة المرتبطة بها (t-sig) بقيمة (٠.٩٥٧)، وأن فقدان الثقة عملية عكسية بالإرهاب السيبراني بوحدة (٠.٠٠٧-) وحده. وقيمة معاملات التضخم Variance Inflation Factors (VIF) ويساوي (١.٠٠٠)، ومعاملات التسامح (Tolerance) ويساوي (١.٠٠٠)، وبالمعادلة حيث VIF = 1 / Tolerance، والتي يتبين منها عدم وجود مشكلة بين المتغيرات حيث كانت معاملات التضخم اقل من (٣).

٢٥- الاستنتاج :

كشفت نتائج الدراسة أن سياسة الخصوصية متشابهة في غالبية مواقع التواصل الاجتماعي، بالإضافة إلى استغلال المعلومات التي تجمعها عن المستخدمين لأن السياسة غير واضحة او غير مفهومة بالنسبة لجميع المستخدمين، وأن تلك الخدمات المجانية ليست في الواقع حقيقة، فهي تستفيد من المعلومات بطريقة أو بأخرى وتستخدمها تجارياً، ونستنتج:

١. أن انتهاك الخصوصية في الإعلام الرقمي يؤدي إلى فقدان ثقة المستخدمين عند شعورهم أن بياناتهم الشخصية تُستغل بطرق غير مشروعة.
٢. يؤدي انتهاك الخصوصية إلى القلق والضغط النفسي مما يسبب تدهور العلاقات الاجتماعية بين المستخدمين ووسائل الإعلام الرقمية، ولذلك يحتاج المستخدمون إلى توعية أكثر بهذا الخصوص.
٣. يؤثر فقدان الثقة الإعلامية في الإعلام الرقمي بطريقة سلبية على سمعة ومصداقية وسائل الإعلام الرقمية ونزاهة المعلومات التي يتم تداولها.
٤. يطالب المختصون في مجال التقنية بضرورة تعزيز الوعي الرقمي لدى الأفراد لحماية خصوصياتهم والتعرف على أخطار انتهاك الخصوصية.
٥. أن الشفافية في تطبيقات وسائل التواصل الاجتماعي بشأن كيفية جمع واستخدام البيانات غير واضحة للأفراد مما يسبب اهتزاز الثقة لدى المستخدمين.
٦. أن التكنولوجيا المتقدمة مثل تقنيات التشفير والحماية السيبرانية غير فعالة وليست كافية لحماية المستخدمين فيجب تشديد العقوبات على المهاجمين والمتطفلين.

٧. تتسبب منصات الإعلام الاجتماعي والتفاعلية بصعوبة التمييز بين المعلومات الصحيحة والمضللة، وأن هناك نقصًا في التحقق من المصادر على الإنترنت.

٨. تتسبب الإعلانات المستهدفة والتي تعتمد على جمع البيانات الشخصية في زيادة قلق المستخدمين بشأن خصوصياتهم وثقتهم في الإعلانات التي يتم عرضها لهم.

٩. أهمية التعليم والتثقيف الرقمي في زيادة الوعي بالمخاطر والتحديات التي تواجه الثقة الإعلامية في الإعلام الرقمي.

١٠. تعمق الشائعات والأخبار المضللة الفجوة بين الأفراد ووسائل الإعلام الرقمية، مما يؤدي إلى زيادة الشكوك وتقليل الثقة في المصادر الإعلامية.

١١. تزايد التجارة الإلكترونية والإعلانات التجارية المتطفلة قد تؤثر سلبًا على الثقة الإعلامية، خاصة عندما يتم تقديم المحتوى الإعلاني دون الشفافية والوضوح.

١٢. هناك تدني في القيم الاجتماعية والثقافية للإعلام الرقمي بسبب نقص المصداقية مما يشكل وجهات نظر مختلفة حول الوسائط الإعلامية الرقمية.

١٣. اعتماد الجمهور على المواقع التفاعلية ووسائل التواصل الاجتماعي وانتشار الشائعات والأخبار المضللة تفقد الثقة بالتكنولوجيا الإعلامية.

٢٦- التوصيات:

انطلاقًا مما سبق:

١. التوعية المجتمعية بمخاطر انتهاك الخصوصية في ظل سياسة إعلامية لتنبيه الجمهور وتوعيته بحقوقه.
٢. إلزام إدارات مواقع التواصل الاجتماعي باحترام الحق في الخصوصية.
٣. إدراج منهج تعليمي حول التربية الإعلامية الرقمية في المدارس والجامعات بكيفية التعامل مع الإعلام الرقمي.
٤. إن تعمل الحكومات والمنظمات والهيئات الرقابية والجهات المعنية على تعزيز قوانين الإعلام وفرض قيود صارمة على المحتوى الضار.
٥. توفير رؤى حول كيفية تحسين السياسات والأنظمة في مجال الإعلام الرقمي لتحديث وتطوير أنظمتها وبرامجها لمواكبة تقنيات الهجمات السيبرانية المتطورة والتصدي لها بشكل فعال.
٦. على الشركات والمؤسسات الرقمية تحسين الحوكمة والشفافية والإفصاح بشأن كيفية استخدام جمع البيانات.

٢٧- الخاتمة:

العنصر البشري للأسف هو الحلقة الأضعف في النظام الأمني وهو المستهدف أيضاً، فتثقيفه عامل أساسي لحماية الخصوصية، وحمايته من الهجمات السيبرانية التي تنبع من التصيد عن طريق رسائل احتيالية بالبريد الإلكتروني، ومن هذا المنطلق، يجب على المستخدمين فهم المبادئ الأساسية للإعلام الرقمي. وفي المملكة العربية السعودية، أصبح المواطن واعياً،

فالحملات التوعوية التي تقوم بها الهيئة الوطنية للأمن السيبراني بنشر التحذيرات الأمنية وتوضيح المخاطر عبر الاعلام الرقمي، واستخدام التحقق الثنائي، وتحديث الأنظمة، وبرامج مكافحة الفيروسات، والجدار الناري، وسد الثغرات الأمنية، أدّى إلى تقليل أثر الهجمات السيبرانية.

ويبقى السؤال، هل يُضحي المستخدم بالخدمات التي تقدمها مواقع التواصل الاجتماعي المتنوعة مقابل الحفاظ على خصوصيته؟ والجواب على السؤال على عاتق المستخدم نفسه. وفي ظل هذا البحث الميداني تبين أن مستخدمي مواقع التواصل الاجتماعي غير مدركين لمخاطر انتهاك الخصوصية، واعتادوا على القبول والموافقة على تقديم بياناتهم الشخصية دون أن يبذلوا جهد في قراءة سياسة الخصوصية بالمواقع التي تكون دائماً طويلة ومعقدة، وبلغة قانونية يصعب على المستخدم فهمها، وهو ما يحمي تلك المواقع من المسؤولية القانونية.

٢٨- المراجع

١.٢٨ الأدبيات:

١- إبراهيم، محمد. (٢٠٢١). " **الحق في الخصوصية الرقمية في إطار ثورة البيانات وأنماط التدخلات التشريعية والدولية**". مجلة البحوث والدراسات الإعلامية. العدد ١٥، المجلد ١٥.

٢- الغيطي، إبراهيم. (٢٠٢١). " **التحديات التي تواجه الصحافة الإلكترونية وسبل معالجتها، دراسة ميدانية على عينة من النخب الأكاديمية المتخصصة**". مجلة البحوث والدراسات الإعلامية. العدد ١٧، المجلد ١٧.

٣. المرشد، لطيفة. (٢٠٢٣). " **الإعلام الرقمي وجهود مكافحة الإرهاب السيبراني) الدور والمعوقات)** ". المجلة المصرية لبحوث الإعلام، العدد ٤٨، ج ٢، أعمال المؤتمر العلمي الدولي ال ٢٤ لكلية الإعلام.

٤. حاجة، أمال. (٢٠٢٣). " **تأثير التطور التكنولوجي وتقنيات الحوكمة الرقمية على السياسة العامة**". مجلة السياسة العالمية، مجلد (٧)، العدد (٢).

٥. سيد، آية. (٢٠٢١). " **إدراك مستخدمي مواقع التواصل الاجتماعي لأهمية الأمن السيبراني ودوره في الأمن المعلوماتي** ". المجلة المصرية لبحوث الإعلام، العدد ٧٧، ج٣، مجلد ٢.

٦. فخرالدين، أريج. (٢٠٢٣). " **الاتجاهات الحديثة في دراسات مخاطر الإعلام الرقمي** ". المجلة المصرية البحوث الإعلام، العدد ٨٤، الجزء ٢.

٧. قرني، أماني. & خطاب، إيمان. (٢٠٢٢). " **دور مواقع الإعلام الرقمي في حماية الأمن السيبراني**". المجلة المصرية لبحوث الإعلام، العدد ٨٠، ج٢.

٨. كدواني، شيرين (٢٠٢٢). " **ضوابط حماية الحق في الخصوصية عبر مواقع التواصل الاجتماعي**". مجلة البحوث الإعلامية. جامعة الأزهر. كلية الإعلام.

٩. عثمان، أحمد. (٢٠٢٣). " **تعرض المراهقين في مصر لوسائل الأعلام التقليدية والرقمية وعلاقته بمفهوم القدوة لديهم** ". المجلة المصرية لبحوث الاعلام، العدد ٨٣ (الجزء الأول).

١٠. عمار، أحمد. (٢٠٢٢). " **استخدام المراهقين لصفحات مكافحة الجرائم الإلكترونية بالفيس بوك وعلاقته بإدارة خصوصيتهم الرقمية**". المجلة المصرية لبحوث الإعلام، العدد ٨١، ج٣.

١١. غريب، سحر. (٢٠٢١). " **إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد في ضوء تأثير الشخص الثالث**". مجلة البحوث والدراسات الإعلامية، العدد ١٨، المجلد ١٨.

١٢.محمدين، أسماء. (٢٠٢٢). " **اتجاهات النخب نحو تشريعات حماية البيانات عبر مواقع التواصل الاجتماعي ودورها في حماية الخصوصية الرقمية لهم**". مجلة البحوث والدراسات الإعلامية، العدد ٢٠، المجلد ٢٠.

١٣.محمد، نرمين. (٢٠٢٢). " **استخدام المراهقين لشبكات التواصل الاجتماعي وعلاقته بإدراكهم لانتهاكات خصوصيتهم**". مجلة البحوث والدراسات الإعلامية، العدد ٢٠، المجلد ٢٠.

٢.٢٨ المواقع الإلكترونية:

١٤.المقرن، أحمد. (١٤٤٥). " **السعودية احتلت المركز ١٣ عالميا والأولى عربيا في الأمن السيبراني**". موقع رسالة الجامعة (https://rs.ksu.edu.sa)،

١٥.موقع تشيك بوينت. (٢٠٢٣). " Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks". (https://blog.checkpoint.com/2023/01/05/38)

١٦.العربية نت. (٢٠١٧) حدثت في (٢٠٢٠). " **تعرف على تاريخ فايروس "شمعون" في السعودية**". موقع العربية (https://www.alarabiya.net/saudi-today/2017/01/24).

١٧.موقع العربية سكاي نيوز. (٢٠٢٣). "**كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟**". موقع العربية (https://www.skynewsarabia.com/business/1670391)

١٨.شومان، محمد. (٢٠١٧). "**لماذا تراجعت ثقة الجمهور في الإعلام؟**" موقع اليوم السابع ، (اليوم السابع(youm7.com)).

١٩.كاسبر سكاي. (بدون تاريخ). " ماهي خصوصية البيانات؟ " الموقع الإلكتروني (الإنترنت والخصوصية الفردية: كيفية حماية نفسك وبياناتك(kaspersky.com))

٢٠.موقع مثابر. (٢٠٢٤) . " تعريف السحابة الإلكترونية". الموقع الإلكتروني (تعريف السحابة الالكترونية وأنواعها ومكوناتها وأهميتها(motaber.com))

٢١. الشامسي، سلطان. (٢٠٢٣). " **خطوات حماية المنظمات من الهجمات السيبرانية** ". موقع مزن الإلكترونية (خطوات حماية المنظمات من الهجمات السيبرانية – منصة مزُن(mozn.ws))

٢٢. المهدي، أماني. (٢٠١٨). " **المجال العام من الواقع الفعلي إلى العالم الإفتراضي معايير التشكل والمعوقات**". موقع المركز الديمقراطي العربي، (https://democraticac.de/)

٢٣. مركز القرار للدراسات الإعلامية. (٢٠٢١). " **المداخل النظرية في بحوث الإعلام الرقمي**". موقع القرار (المداخل النظرية في بحوث الإعلام الرقمي – مركز القرار للدراسات الإعلامية(alqarar.sa)).

٢٤. حسن، نسرين. (٢٠٢١). " **الثقافة الرقمية، رؤية تحليلية**". موقع خطوة للتوثيق والدراسات، (الثقافة الرقمية .. رؤية تحليلية – مركز خُطوة للتوثيق والدراسات (khotwacenter.com)).

٢٥. المجدوب، أحمد. (٢٠١٩). " **نصائح لاستخدام التكنولوجيا** ". موقع عين ليبيا. (نصائح لاستخدام التكنولوجيا(eanlibya.com)).

٢٦. سايبر أرابز. (٢٠١٧). " **أنواع البرمجيات الخبيثة التي تهددك إلكترونياً**". موقع سايبر أرابز، (https://cyber-arabs.com/).

٢٧. المراقب. (٢٠٢٣). " **الخوارزميات ومواقع التواصل الاجتماعي، وكيف تعمل**". موقع المراقب، (https://almourakeb.net/).

٢٨. أوراكل. (بدون تاريخ). " **الذكاء الاصطناعي مقابل التعلم الآلي**". موقع أوراكل، (https://www.oracle.com/sa-ar/artificial-intelligence).

٢٩. فاستر كابيتال. (٢٠٢٤). " **تتبع نظام تحديد المواقع العالمي GPS**". موقع فاستر كابيتال، (https://fastercapital.com/arabpreneur/).

٣٠.سكاي نيوز عربية. (٢٠٢٣). " **كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟**". موقع سكاي نيوز عربية، (https://www.skynewsarabia.com/business/).

٣١.مركز القرار للدراسات الإعلامية. (٢٠٢٣). " **استراتيجيات الاتصال التسويقي ومستقبل صناعة المحتوى في الإعلان الرقمي**". موقع القرار، (استراتيجيات الاتصال التسويقي ومستقبل صناعة المحتوى في الإعلان الرقمي – مركز القرار للدراسات الإعلامية(alqarar.sa)).

٣٢.خلدون، غسان. (٢٠٢٠). " **تقنيات متطورة للتعرف على الوجوه**". موقع الشرق الأوسط الإلكترونية، (تقنيات متطورة للتعرف على الوجوه(aawsat.com)).

٣٣.مبروك، إيمان. (٢٠٢٤). " **ما تأثير تغيير إجراءات التتبع لغوغل على الإعلام**". موقع الشرق الأوسط الإلكترونية، (ما تأثير تغيير إجراءات التتبّع لـ«غوغل» على الإعلام؟(aawsat.com)).

٣٤.مركز القرار للدراسات الإعلامية. (٢٠٢٢). " **التسويق الفيروسي عبر منصات التواصل الاجتماعي**". موقع القرار ("التسويق الفيروسي" عبر منصات التواصل الاجتماعي – مركز القرار للدراسات الإعلامية(alqarar.sa)).

٣٥.كاسبر سكاي. (بدون تاريخ). " **كيفية حماية خصوصيتك على الإنترنت في الاستخدام الشخصي او المهني**". موقع كاسبر سكاي، (نصائح للمحافظة على الخصوصية على الإنترنت(kaspersky.com)).