إدراك الصحفيين للمخاطر الرقمية وإستراتيجيات تطبيقهم للأمن الرقمي في عملهم المهني

د. وسام محمد أحمد حسن

مدرس بقسم الصحافة - كلية الإعلام
جامعة الأهرام الكندية

مقدمة:

فرضت التطورات التكنولوجية على الصحفيين العمل عبر المنافذ الرقمية؛ سواء في جمع المعلومات والتحقق منها، أو في التواصل مع المصادر، أو استقبال وإرسال وتخزين عملهم إلكترونيًا، ويكمن مبدأ سلاسة وتكامل التفاعل الرقمي في جوهر الأمن تجاه استخدامات التقنيات الحديثة، بعد أن أصبح العالم متصلا رقميًا بصورة مثيرة، وبعد سنوات من الحديث عن النفاذ الرقمي، وضرورة تهيئة البنية التحتية في المجتمعات، من أجل تمكين كل الفئات من الحق في النفاذ إلى خدمات الاتصالات، ومنع الإقصاء الرقمي؛ أثيرت شواغل الاتجاهات الدولية تجاه الأمن الرقمي، وتمثلت أهمية هذا الاتجاه في اهتمام الدول بصياغة بنود في قوانينها تكفل هذه الحقوق، وتبني المؤسسات الدولية والمحلية مبادرات للتوعية بالأمن الرقمي.

وقدمت مجموعات متنوعة من المنظمات والمؤسسات مبادرات تدريبية؛ لرفع الوعي بالأمن الرقمي؛ سواء للصحفيين أو لغير الصحفيين، بالإضافة إلى المساهمة في وضع نهج شامل لمناهج تدريبية عن الأمن الرقمي، يفيد منها الأكاديميون أو العاملون في مجال الإعلام، ويقصد بالأمن الرقمي هنا الإستراتيجيات والأدوات التي يمكن للفرد استخدامها لتأمين خصوصيته، وحماية هويته، عبر تقييد إتاحة البيانات لأشخاص أو مؤسسات معينة، والحفاظ على أجهزته ضد الاختراق أو السطو أو الإتلاف من قبل مستخدم خارجي؛ سواء كان برمجيات ضارة وفيروسات، أو أفرادًا وجهات تستهدف جمع بياناته أو تتبعه.

ومن الأمثلة التي تدلل على أهمية الأمن الرقمي، لا سيما وأن الصحفيين تتهددهم مخاطر بحكم المهنة، تتمثل في محاولة الاختراق الإلكتروني والتقصي، أن أوصت **اليونسكو** بتضمين مناهج لسلامة وأمن الصحفيين في عدة أبعاد؛ منها الأمن الرقمي، بحيث تهدف إلى التوعية بالأدوات اللازمة للحد من نقاط الضعف، والتهديدات الرقمية، والهجمات السيبرانية، والتطفل الرقمي[1]، وقدمت منحًا سنوية لمبادرات سلامة الصحافة، ونظمت دورات تدريبية عبر الإنترنت خاصةً بالأمن الرقمي، فضلا عن دعمها لمؤشرات السلامة التي تشمل بعدًا رقميًا، كما نظمت، بالتعاون مع **معهد تقارير الحرب والسلام**، سلسلة من الدورات التدريبية في مجال الأمن الرقمي للصحفيين التونسيين، ونظمت مؤسسة **''رايتس كون RightsCon''**، المعنية بحقوق الإنسان في العصر الرقمي، عدة مؤتمرات هدفت إلى رفع الوعي، وتقديم المشورة الأمنية الرقمية، والتدريب على تطبيق أدوات الأمان الرقمية[2]، وأطلق **"مجلس البحوث والتبادلات الدولية IREX''** مبادرة **"أمن SAFE"**؛ لتمكين العاملين في مجال الإعلام، وتدريبهم على الوسائل والأدوات اللازمة للأمن الرقمي والسلامة للصحفيين، وقدم منهجًا إرشاديًا لتدريب الصحفيين على الأمن بأربع لغات[3]، كما دشن **''معهد صحافة الحرب والسلام''** موقعًا خاصًا بالأمن الرقمي في العالم العربي **Cyber-Arabs**، يهدف إلى رفع الوعي بالأمن الرقمي، وإرشاد الجمهور إلى كيفية المحافظة على أمنهم أثناء عملهم على شبكة الإنترنت[4].

ومن المبادرات العربية **''دليل البقاء للصحفيين – Journalist Survival Guide"**، الذي أصدره **"مركز الدفاع عن الحريات الإعلامية والثقافية بلبنان''**، والذي تم إطلاقه عبر موقع وسائط متعددة تعليمي[5]، ومن المبادرات الدولية الأخرى التي توفر دليلا لمنهج تدريبي للأمن الرقمي **"مؤسسة إنترنيوز Internews"**[6]، وعلى المستوى الأكاديمي اعتمدت **''كلية الصحافة في جامعة كولومبيا''** برنامجًا دراسيًا جديدًا، يسعى إلى تحليل المخاطر الرقمية، وتعزيز أساسيات الأمن الرقمي للصحفيين، ونسقت **"جامعة نيويورك''** ورش عمل للتدريب على الأمن الرقمي لطلاب

الدراسات العليا، وقدم "**مركز Knight Center**" ندواتٍ عبر الإنترنت حول قضايا السلامة الرقمية[7].

وفي مصر، اهتمت **وزارة الاتصالات وتكنولوجيا المعلومات** برفع الوعي بأهمية الأمان على الإنترنت؛ فقدمت الإستراتيجية الوطنية للأمن السيبراني؛ وصاغت عددًا من الأدلة الخاصة بالأمان الإلكتروني للأسرة؛ وتبنت المبادئ التوجيهية لحماية الأطفال على الإنترنت، التي صاغها الاتحاد الدولي للاتصالات، بالإضافة إلى تقديم عدة أدلة خاصة بتوعية الأفراد باستخدام مواقع التواصل الاجتماعي، وإدراك الخصوصية والآثار الرقمية وإدارة السمعة في العصر الرقمي، كما وضعت قضايا السلامة على الإنترنت في مقدمة أعمال التعاون مع المجتمع الدولي؛ (مثل التعاون مع منتدى حوكمة الإنترنت، والاتحاد الدولي للاتصالات، واليوم العالمي للإنترنت الآمن، وتحالف المنظمات الأوروبية غير الحكومية العاملة في مجال سلامة الإنترنت)[8].

ولا تقتصر المخاطر الأمنية التي يتعرض لها الصحفيون والمؤسسات الصحفية على الملاحقات القضائية، ففي عام 2013 فقط، كشفت مجموعة كبيرة من المؤسسات الصحفية، منها (نيويورك تايمز، وصحيفة وول ستريت جورنال، وصحيفة بلومبرج، وواشنطن بوست) عن أن أنظمة الاتصالات الرقمية الخاصة بها كانت هدفًا لهجمات رقمية، وقد بدا في بعض الحالات أن الهدف هو كشف مصادر الصحفيين، إذ أشار توقيت الهجوم ونمطه على صحيفة نيويورك تايمز أن الدافع كان الكشف عن هوية المصادر لمجموعة من القصص المرتبطة بمسئولين حكوميين صينيين، وفي حالات أخرى، بدت مظاهر القرصنة أوضح عندما قام الجيش السوري بتشويه موقع فايس VICE، بعد نشر قصة كشفت عن هوية حقيقية لأحد الأفراد، كما تم اختراق حساب تويتر الخاص بوكالة الأسيوشيتدبرس، لبث تقارير كاذبة عن انفجار بالقرب من البيت الأبيض[9].

ومن أبرز الحالات التي يمكن الحديث عنها، باعتبارها مثالا لحاجة الصحفيين للوعي بالأمن الرقمي، ما ورد في تسريبات **إدوارد سنودن**، الموظف التقني

السابق في وكالة الأمن القومي الأمريكية NSA، لعديد من الوثائق في عام 2013، حول قيام الوكالة بجمع سجلات المكالمات الهاتفية لملايين المواطنين[10]، بالإضافة إلى محاولات وكالة الأمن القومي تقويض برامج الخصوصية والأمن، مثل اعتراض متصفح شبكات تور Tor، (هي شبكات توفر حماية للخصوصية يعتمد عليه الصحفيون والنشطاء في مجال حقوق الإنسان في عديد من الدول، مثل الولايات المتحدة وأوروبا، وكذلك الصين وروسيا وإيران؛ للحفاظ على خصوصية اتصالاتهم)، مما يمنح الوكالة السيطرة الكاملة على أي جهاز كمبيوتر يستخدم هذا المتصفح، وجمع بيانات اتصالاته وأعماله، وهو ما يشكل تهديدًا أمنيًا كبيرًا للصحفيين[11]، بالإضافة إلى إطلاق الوكالة لبرنامج تجسس رقمي، يدعى بريسم Prism، حيث تقول الوثيقة المسربة إنه يسمح للوكالة بالولوج إلى خوادم (سيرفرات) الشركات التكنولوجية الكبرى، وجمع البيانات، بما في ذلك سجل البحث ورسائل البريد الإلكتروني وعمليات نقل الملفات والمحادثات الحية؛ وتدعي الوثيقة أن جمع هذه البيانات يتم مباشرة من الخوادم المقدمة للخدمة، وعلى الرغم من أن الوثيقة تشير إلى علم هذه الخوادم بالمعلومات التي يتم جمعها، فإن هذه الشركات نفت معرفتها ببرنامج من هذا القبيل[12]، ورغم أنه لم يكن فيما كشفه سنودن ما يشير إلى أن الصحفيين كانوا أهدافًا خاصة، فإن هذا الكشف مثّل صدمة لمجتمع الصحافة الأمريكي على وجه الخصوص، الذي كان يعتقد أن اتصالات الصحفيين مع المصادر محمية بشكل فعال من تدخل الحكومة، من قبل ما يسمى "قوانين الردع"shield laws، التي تمنع إجبار الصحفيين على الكشف عن مصادرهم، كما أشارت وثائق سنودن إلى وجود تسلل حكومي إلى أنظمة شركات الاتصالات، التي قامت العديد من المؤسسات الصحفية بعقد شراكة معها لإمدادها بخدمات البريد الإلكتروني، مما زاد من معدل القلق تجاه الخصوصية[13].

ومن الأهمية الإشارة إلى أن الصحفي جلين جرينوالد، الكاتب بصحيفة الجارديان وأحد المدافعين عن الحقوق والحريات والذي وقع اختيار سنودن

عليه كي يكشف له عن الوثائق السرية، طلب منه سنودن أن يحصل على مفتاح PGP (دالة تشفير للبريد الإلكتروني، وتتكون من زوج من المفاتيح؛ عام وسري)، كي يتمكن من إرسال بريد إلكتروني آمن إليه، ولم يكن جرينوالد يفهم ما المقصود، وكاد أن يتجاهل هذه الرسالة، خاصة أنه لم يكن يعرف المصدر، فما كان من سنودن إلا أن أرسل إليه برنامجًا تعليميًا حول التشفير؛ كي يتمكن من إرسال الرسالة إليه[14]، وهو ما أدى إلى تأجيل الكشف عن الوثائق السرية لحين إيجاد طريقة آمنة للتواصل، بينما كانت المخرجة لورا بويتراس، مخرجة فيلم "المواطن الرابع"، وهو فيلم وثائقي يدور حول إدوارد سنودن، لديها مفتاح PGP، مما جعل إجراء محادثة آمنة معها أسهل[15]، وهو ما يبرهن على أهمية استخدام الأدوات الآمنة أثناء الاتصال بالإنترنت، خاصة فيما يتعلق بتناول موضوعات حساسة، في ظل ازدياد الاعتماد على تكنولوجيا الاتصال في غرف الأخبار، واعتبار الإنترنت مكان اجتماع افتراضي للأفراد، للتواصل وتبادل المعلومات والأفكار، ومناقشة القضايا الهامة، بما فيها الصحفيون ومصادرهم.

مشكلة الدراسة:

المجتمع الذي يعمل فيه الصحفي اليوم هو نتاج انصهار التكنولوجيا وإتاحتها في المجتمع، عبر عديد من التطبيقات التكنولوجية المرتكزة على الإنترنت، والتي أصبحت تختصر المسافات، وتقلل الوقت والجهد؛ وفي أي مجتمع يتفاعل فيه الأفراد ينبغي أن تكون هناك مجموعة من القواعد الحاكمة والمنظمة، والأطر الموضوعة لضمان السلامة، إلا أن مجتمع الإنترنت يشهد تفاعلات وممارسات قد تكون مخيبة للآمال في بعض الأحيان، وتنبئ عن مخاطر، مثل الجرائم الإلكترونية، والرقابة السيبرانية، والتتبع، والوصول إلى معلومات لا يرغب الفرد أن يعرفها آخرون، بالإضافة إلى ممارسات الإرهاب الإلكتروني.

لذلك يعتبر الأمن الرقمي قضية مطروحة بقوة على الساحة الإعلامية مؤخرا، بسبب تنامي المستحدثات الرقمية، كأدوات داعمة للتواصل وللحصول على

المعلومات من جهة؛ والحاجة إلى رفع ثقافة الأمن السيبراني من جهة أخرى، مما يؤدي إلى التغلب على أي مخاطر محتملة، والصحفيون ليسوا بمنأى عن هذه المخاطر، مما يجعل من الضروري فهم ووعي المسئوليات المتعلقة بالحد من إمكان تتبعهم وحماية أجهزتهم، وإكسابهم مزيدًا من الخصوصية والحماية، عبر التوعية والتدريب على الأمن الرقمي، وهو ما ينبغي أن ينعكس أيضا على مبادرات تفعيل منظومة الأمن السيبراني للمؤسسات الصحفية؛ سواء لحماية أصولهم الإلكترونية، أو لمساعدة صحفييهم في العمل بأمان.

ومن هنا تتلخص مشكلة الدراسة في معرفة مستوى استخدام المبحوثين للأجهزة والتطبيقات الرقمية المختلفة، ورؤيتهم لطبيعة المشكلات التي تتعلق بالأمن الرقمي، ومعرفة نماذجهم الذهنية للمخاطر والتهديدات الرقمية المحتملة، وتأثيرها على الإستراتيجيات والتدابير التي ينتهجونها من أجل تعزيز أمنهم الرقمي، بالإضافة إلى التعرف على دور مؤسساتهم الصحفية في دعم الأمن الرقمي وتدريبهم على إدارة السلوك التكنولوجي، بما يحقق لهم الأمن أثناء ممارسة مهنتهم عبر الوسائط التكنولوجية والإنترنت.

أهمية موضوع الدراسة:

1. تتناول هذه الدراسة بُعدًا جديدًا، وهو الأمن الرقمي؛ حيث تفيد في تحديد مستويات الوعي، وتحديد إستراتيجيات الأمن الرقمي للصحفيين، في ظل تنامي الاعتماد على التكنولوجيا والأدوات الرقمية، وازدياد استخدام الصحفيين للوسائل التقنية المرتبطة جميعها بشبكة الإنترنت.

2. مع تصاعد وتيرة الجرائم الإلكترونية والإرهاب الرقمي والتطفل على بيانات الأفراد؛ تظهر حاجة الصحفيين إلى تحقيق الوعي المطلوب؛ سواء لحماية أنفسهم، أو لحماية مصادرهم، لذلك يعد رفع الوعي، وتنسيق آليات التدريب، ظاهرةً صحيةً، ينبغي على المؤسسات الصحفية أن تنتهجها وأن تتبناها؛ بعد أن أصبحنا نشهد اليوم شركات خاصة تقدم خدماتها للمؤسسات الصحفية، لمساعدتها حال التعرض لاختراق، وشركات أخرى

تحت مسمى (خبراء التحقق في الكمبيوتر والأدلة الرقمية)، مما أصبح لزامًا على المؤسسات أن تُعنى بحماية حساباتها، وحماية صحفييها، كتحدٍّ جديد في العالم الرقمي، وهو ما تحاول هذه الدراسة تسليط الضوء عليه.

3. تستمد الدراسة أهميتها من تأكيد المنظمات المختلفة على أهمية الأمن الرقمي، حيث تتوفر عدة أدلة توجيهية خاصة بالأمن الرقمي، لتعظيم الاستفادة من التكنولوجيا، وزيادة استثمار استخداماتها، مع رفع مستوى الأمان بنسبة كبيرة؛ إلا أن مستوى هذه الأدلة الاسترشادية معقد ومتقدم إلى حد ما، وبحاجة إلى تبسيط، وتعاون بين المؤسسات الصحفية والجهات التكنولوجية.

4. الحاجة إلى إجراءات وقائية تجاه الأدوات الرقمية؛ لتعظيم الاستفادة المثلى من مميزاتها وإيجابياتها، وتقليل المخاطر قدرً الإمكان، ولذلك تتمثل أهمية الدراسة في تسليط الضوء على مهارات التعامل مع الوسائل والأدوات الرقمية، بما يحقق الأمن الرقمي، ويقلص من بيانات البصمة الرقمية، ويواجه التهديدات السيبرانية.

أهداف الدراسة:

يتمثل الهدف الرئيسي للدراسة في معرفة إدراك الصحفيين بإستراتيجيات الأمن الرقمي والتحديات المرتبطة به، وطرق التقليل من المخاطر الرقمية أثناء الممارسات الرقمية المختلفة على أجهزة الكمبيوتر والهواتف المحمولة واستخدام الإنترنت، وذلك من خلال:

1. التعرف على مستوى استخدام الصحفيين للوسائل والأدوات الرقمية.
2. التعرف على المخاطر والتهديدات الرقمية من وجهة نظر الصحفيين.
3. الكشف عن الممارسات الأمنية الرقمية الخاصة بالصحفيين.
4. التعرف على التحديات التي تواجه الصحفيين من أجل ممارسات أمنية رقمية قوية.
5. معرفة الدور الذي تلعبه المؤسسات الصحفية في توعية وتدريب الصحفيين على الأمن الرقمي.

الإطار النظري للدراسة:

النموذج العقلي (Mental Model) والممارسات الأمنية للصحفيين:

كان أول من تحدث عن النماذج العقلية عالم النفس الإسكتلندي **كينيث كرايك Kenneth Craik** عام 1943، في كتاب "طبيعة التفسير"، حيث قدم افتراضًا بأن العقل يبني نماذج صغيرة للواقع، يتم استخدامها لأسباب مختلفة، مثل استباق الأحداث والتنبؤ بها، أو تأكيد التفسيرات التي تدور في ذهن الفرد، واقترح **جونسون لايرد Philip Johnson-Laird** بعد ذلك، في عام 1989، أن النماذج العقلية يخلقها القارئ تجاه النص الذي يقوم بقراءته، من أجل أن يحاكي العالم الموصوف في كلمات النص، من خلال ما يفهمه أو يفسره هو؛ وفقا لخبراته وتجاربه؛ ووفقًا لهذا الافتراض يمكن أن تؤدي الفقرات الغامضة بنص ما إلى أكثر من تصور عقلي لدى كل قارئ، وهو ما يعتمد عليه مؤلفو الرواية لإبقاء القارئ في حيرة من أمره، وعدم إعطائه تصورًا مباشرًا لتسلسل الأحداث أو للنهاية[16].

ويعني ذلك أن النماذج العقلية توضح كيف يقوم الفرد بالاستدلال لمشكلة أو موقف ما؛ من خلال التفكير فيه، وطرح رؤى وتفسيرات له، واتخاذ قرارات بشأنه وفقا لما يعتقده ويتصوره تجاه هذا الشيء، لذلك فهو يختبر واقعه عبر معرفته المسبقة وتصوراته الخاصة.

وتم تطوير هذا النموذج على يد جونسون لايرد Johnson Laird وروث بايرن Ruth Byrne، حيث ذهبا إلى أن هناك عدة أنواع من التمثيلات العقلية، مثل (التصورات العقلية mental models، والارتباطات الإدراكية لهذه التصورات prepositional representations، والصور images التي تعد الارتباطات الذهنية للنماذج العقلية)، لذلك فإن الأفراد لا يعتمدون بشكل أساسي على قواعد الاستدلال، ولكنهم يعتمدون على نماذجهم الذهنية (تصوراتهم العقلية)، التي تستند على فهمهم للمعاني ومعارفهم العامة، لذلك يعتبر المبدأ الأساسي لهذه النظرية أن الأفراد يمثلون أقل قدر ممكن من المعلومات في النماذج الواضحة[17].

ويرى بعض الباحثين أن النماذج الذهنية يمكن أن تكون مفيدة في

فهم سلوك الأمن الرقمي، حيث يمكن أن تكون هناك اختلافات كبيرة بين التصورات العقلية للمستخدمين ذوي المعرفة البسيطة بالتكنولوجيا، والمستخدمين ذوي المعرفة المتقدمة، الذين يدركون المخاطر الرقمية بشكل مختلف، وبالتالي تتشكل لديهم تصورات مختلفة تجعلهم يستجيبون في النهاية بطرق مختلفة[18].

ومن أبرز تعريفات النموذج العقلي وصفه بالبناء الذي يستخدمه الفرد لتمثيل النظام واتخاذ القرارات بشأنه[19]، حيث إن التصورات الذهنية غير مكتملة، وقدرات الأفراد على محاكاة أو تنفيذ تصوراتهم قد تكون محدودة للغاية، وقد تكون غير مستقرة حيث ينسى الفرد تفاصيل النظام الذي يستخدمه، خاصة عندما لا يتم استخدام هذه التفاصيل لفترة ما[20].

وقد استخدمت النماذج العقلية على نطاق واسع في التفاعل بين الإنسان والحاسوب، وسهولة الاستخدام، حيث تعتبر قابلية استخدام النموذج المفاهيمي للتصميم ووظائفه، وإمكانية تعلمه تعتمد على التوافق بين النموذج التصوري للتصميم، والنماذج الذهنية للمستخدمين[21].

ويمكن التفرقة بين النماذج المفاهيمية Conceptual Models، وبين النماذج العقلية Mental Models، فالنماذج المفاهيمية هي أدوات لفهم النظم المادية، أما النماذج العقلية فهي ما يمتلكه الأفراد حقا في عقولهم أو تصوراتهم، وعلى سبيل المثال: **(يمكن أن يتكون النموذج الذهني لاستخدام محركات البحث للحصول على المعلومات عبر الإنترنت من: أ- نموذج ذهني يصور للفرد كيفية استرجاع محرك البحث للمعلومات وتصنيفها، ب- ونموذج مفاهيمي حول مفردات كلمات البحث التي يمكن أن تحقق نتائج أفضل)**، هذه النماذج مجتمعة تشكل النموذج الذهني للمستخدمين حول البحث على الإنترنت[22]. **ورغم أن كثيرًا منا قادر على استخدام نماذج مفاهيمية مختلفة جيدة للبحث في محرك البحث جوجل للحصول على معلومات، فإن النماذج العقلية الخاصة بكيفية عمل خوارزميات البحث الخاصة بمحرك البحث معقدة الفهم بالنسبة للفرد، وهو لا يشغل بالا بكيفية عملها**، مما يعني أن النماذج التي تساعد في تكوين

نموذج عقلي (ذهني أو مفاهيمي) ليست دائمًا وافية أو دقيقة؛ مما يقلل من فعالية النموذج العقلي، لكنه لا يجعله عديم الفائدة تماما، مما يعني، في هذا المثال، أنه يمكن للفرد أن يحصل على الفائدة من استخدام محرك البحث عبر نموذج مفاهيمي فقط وليس ذهنيًا، لذلك من الممكن أن يكون لدى المستخدمين نماذج عقلية تستند على نماذج غير مكتملة، لكنها لا تزال كافية للاستخدام، علاوة على ذلك؛ لا تترجم تجربة الفرد لنظام ما، بالضرورة، امتلاكه نموذجًا عقليًا تجاهه، فعلى سبيل المثال، وجدت الأبحاث الخاصة بالنماذج العقلية للمستخدمين على شبكة الإنترنت أن كثيرًا منهم استخدمه على نطاق واسع وفعال للأغراض المرجوة، إلا أن غالبيتهم لا يمتلكون نموذجًا عقليًا كاملا ومفصلا لكيفية عمل الإنترنت، وقد أدى ذلك إلى استنتاج أن الاستخدام المتكرر للإنترنت يبدو ضروريًا أكثر من كونه شرطا كافيا لإيجاد نماذج ذهنية مفصلة[23]، وتتغير النماذج الذهنية وتتطور بمرور الوقت، وتتكيف مع المعلومات الجديدة والخبرات المختلفة التي يكتسبها الأفراد[24].

وتطبيقًا لهذا المفهوم، يمكن القول بأن النموذج العقلي يعني وجود تفاهمات وممارسات أمنية للصحفيين، خاصة بالأنظمة التكنولوجية المتعلقة بالأمن الرقمي، التي قد يكون لدى الصحفيين أنفسهم مستويات مختلفة من فهمها، لذلك فإن استكشاف وتوصيف النماذج الذهنية للصحفيين لأمن المعلومات يساعد في توضيح لماذا يتخذ الصحفيون خيارات أمن المعلومات التي يقومون بها[25].

بمعنى أنه قد يكون هناك مجموعة من الاختلافات بين المعتقَد والممارَس؛ فما يعتقده الصحفي من مخاطر، أو ما يعتقده من أساليب محددة قد توفر له الأمن، ليس بالضرورة أن يؤكده بالممارسة، لذلك فإن جوهر النماذج العقلية والممارسات الأمنية للصحفيين، التي تختبرها هذه الدراسة، يتحدد في مدى إدراكهم العقلي للمخاطر المتوقعة والتهديدات المرتقبة، ومعرفتهم بالأدوات التي تتيح لهم تعزيز الأمن، وانعكاس ذلك على إستراتيجيات محددة يقومون بها لحماية أمنهم، حيث يمكن القول بأن النماذج الذهنية يمكن أن تعطي فهمًا لدوافع الأفراد وعمليات التفكير.

وتضع الدراسة مقياسًا حول معرفة الصحفيين بمجموعة من الأدوات، التي يمكن أن تعزز أمنهم الرقمي، ومقياسًا للإستراتيجيات الفعلية التي ينتهجونها، من أجل اختبار العلاقة بين معرفة الصحفيين بأدوات الأمن الرقمي وبين الإستراتيجيات التي يتبنونها، كما تفترض الدراسة أن تحسين الفهم واتخاذ الموقف تجاه الأمن الرقمي، يأتي من خلال النماذج العقلية التي يشكلها الفرد حول المخاطر والتهديدات المحتملة، التي من شأنها أن تكون ضارة بالنسبة إليهم، وهي بذلك تطرح تساؤلا حول ما يدركه الصحفيون حول المخاطر والتهديدات الرقمية.

ويرى البعض أن الوسيلة الأفضل لتحقيق الأمن هي **الأمن من خلال الغموض** Security by Obscurity Model، ويعني ذلك تجنب ما يتعلق بتكنولوجيا الاتصالات الرقمية، فيفترض نموذج الأمن من خلال الغموض، حسب ما اقترحه كل من McGregor and Watkins[26]، اعتقاد الصحفيين أن سبيل الحماية يكون من خلال العمل على الأخبار غير الحساسة، وغالبًا ما يعتقدون أن التهديدات الأهم ليست رقمية، بل قانونية في المقام الأول، وبالتالي فهم يؤكدون ضرورة حماية أنفسهم من مقاضاتهم بتهم مثل التشهير، ويعتبر هذا النموذج أن لدى الصحفيين تصورًا ذهنيًا غير مكتمل للتهديدات الرقمية، حيث لا ينكرون أن الحكومات قد تمارس الرقابة عليهم، أو تستهدفهم، لكنهم لا يرون أن ذلك يتعارض مع عملهم، وبينما يستهدف المتسللون الرقميون الأشخاص ذوي الأهمية، أو ما يطلق عليهم الأسماك الكبيرة، حيث إنه من غير المحتمل أن يكون الأفراد هدفًا للمتسللين إذا لم يكونوا محل أهمية؛ فبالتالي يكون الأفراد الأقل أهمية أكثر أمنًا من القرصنة والهجمات الرقمية، فعلى سبيل المثال يمكن أن يكون مسئول تنفيذي في أحد البنوك الكبيرة هدفًا للمتسللين الرقميين أكثر من موظف لا يشغل أي منصب[27]، ويعني ذلك أن العمل الصحفي، بصفة عامة، قد يكون من الأعمال التي تجذب المتسللين الرقميين إلى محاولة اختراق واعتراض الأشخاص القائمين عليه، إلا أن هذا الاختراق لن يكون لجميع الصحفيين، ولكنه قد يكون للصحفيين الذين يقومون بالعمل على

قصص حساسة، أو يتواصلون مع مصادر هامة، مما يزيد من تعرضهم لمخاطر الهجمات الرقمية.

بينما يعتقد البعض أنه يمكن تحقيق الأمن عن طريق اعتبار **الأمن كفرصة** Security as Opportunity، حيث تشير الفرصة هنا إلى اعتقاد الصحفيين بأن الأمن يتيح لهم فرصة العمل على القصص التي قد لا يتمكنون من العمل عليها دون تحقيق عنصر الأمان بشكل مثالي، ولهذا السبب يواصلون تثقيف أنفسهم حول التهديدات الرقمية وأساليب الحماية والتقنيات الجديدة، وهم بهذه الصورة ليسوا محدودين في العمل على نوع قصص معين، مثل المجموعة الأولى ''الأمن من خلال الغموض''، التي لا تعمل إلا على القصص غير الحساسة[28]، وسوف تستفيد الباحثة من هذه التصنيفات في تحليل النتائج الخاصة بمقياس الإستراتيجيات المستخدمة في تعزيز الأمن الرقمي للصحفيين.

الدراسات السابقة:

ظهرت في السنوات الأخيرة بحوث هامة حول التهديدات الأمنية الرقمية، التي يواجهها الصحفيون العاملون في مناطق مختلفة من العالم، باعتبار أن التحرر من الرقابة الرقمية أمر حيوي لحرية الصحافة، مما يجعل الأمن الرقمي مجالا يجدر الاهتمام به، ولا يقل عن الأبعاد القانونية لحرية الصحافة، أو الأمن الجسدي المرتبط بالسلامة المهنية، هذا بالإضافة إلى إصدار عديد من الأدلة الاسترشادية والتعليمية للحماية والأمن الرقمي، ومن أهمها دليل اليونسكو، الذي تضمن أيضًا توصيفًا لدمج السلامة الرقمية في مقررات الصحافة، وأدلة الاتحاد الدولي للاتصالات، ودليل الأمن الرقمي وحماية المعلومات والحق في استخدام شبكة آمنة، الصادر عن مركز هردو لدعم التعبير الرقمي.

وتعرض الباحثة الدراسات السابقة من خلال ثلاثة محاور؛ المحور الأول حول دراسات الأمن الرقمي للصحفيين، التي اهتمت بالتعرف على إدراك الصحفيين للمخاطر الرقمية المرتبطة بالعمل الصحفي، واستخداماتهم

لتقنيات الأمن الرقمي، والمحور الثاني حول الدراسات التي اهتمت بصياغة إرشادات الأمن الرقمي، والدراسات التي أجريت حول أحد عناصر الاتصالات الآمنة، بينما تركز دراسات المحور الثالث على علاقة النموذج العقلي بدراسات الأمن الرقمي، التي كانت في أغلبها مرتبطة بأمن الكمبيوتر وحماية الخصوصية، بالإضافة إلى بعض الدراسات المرتبطة بمصادر المعرفة المكتسبة للأمن الرقمي.

المحور الأول: دراسات الأمن الرقمي للصحفيين:

بعد أن كان الصحفيون أهدافًا للهجمات الجسدية، أصبحوا اليوم أهدافًا للهجمات الرقمية، ففي دراسة حول مخاطر إنترنت الأشياء IoT على الصحفيين (Shere A., et. al. 2020)[29]، والأساليب الوقائية التي يمكن أن يكون لها فعالية في زيادة أمنهم السيبراني ضد جميع التهديدات الإلكترونية؛ أوضحت النتائج أن الصحفيين، بشكل عام، لا يدركون المخاطر المتعلقة بإنترنت الأشياء، ولا يحمون أنفسهم بشكل كاف، رغم أن الوصول غير المصرح به إلى جهاز واحد، يمكن أن يسمح للمهاجمين باختراق بيئة ذكية بأكملها، مما قد يتسبب في ضرر مادي لبيئته، فضلا عن التسلل لبيانات المستخدم، كما أوضحت النتائج أن الصحفيين والمؤسسات الصحفية يقومون بطلب المساعدة من مستشاري الأمن الرقمي بعد تعرضهم للهجوم، وكان النهج الأساسي الذي يميل إليه بعض الصحفيين تجاه حماية أنفسهم هو النهج التقليدي، من حيث تقليل التفاعلات مع أجهزة إنترنت الأشياء، والعودة إلى الأساليب التقليدية لجمع البيانات والتواصل والتخزين، رغم ما يرون في ذلك من صعوبة، ويتوقع خبراء الأمن الرقمي أن الجمهور، بما فيهم الصحفيون، لن يتمكنوا من إلغاء تفاعلهم، وجعل معلوماتهم عرضة لإنترنت الأشياء خلال السنوات الخمس المقبلة.

لذلك يقترح الخبراء بعض الحلول قصيرة المدى، التي يمكن تركيز الجهود عليها، بما يحد من قدرة أجهزة إنترنت الأشياء على جمع المعلومات الشخصية، وتتضمن هذه الإجراءات اختيار كلمات مرور قوية، وتفعيل جدران الحماية، وتجنب الشبكات اللاسلكية العامة، وتعمد إدخال بيانات

غير صحيحة عن المستخدم لحماية الخصوصية في حال الاختراق، ويرى الصحفيون أن الجهات التي ينبغي أن تساهم في تعزيز أمنهم الرقمي هي المؤسسات الصحفية والنقابات، دون محاولة إشراك شركات التكنولوجيا في مسئولية حماية الصحفيين، حيث يعتبرون أن التكنولوجيا، بصفتها صناعة، تميل إلى أن تكون أكثر انسجامًا مع مصالح الدولة، حيث يرى الصحفيون أن كثيرًا من التهديدات يأتي من قبل الحكومات.

وعندما يحتاج الأفراد إلى اتخاذ قرارات بشأن الأمان الرقمي، فإنهم يعتمدون على تصوراتهم للتهديدات أو المخاطر المحتملة، فوفقًا لدراسة حول إدراك الصحفيين للتهديدات الرقمية، وإدراكهم لأدوات وتقنيات التواصل بشكل آمن، أجريت دراسة (Tsui L., and Francis L., 2019)[30] على الصحفيين في هونج كونج، وذهبت النتائج إلى وجود اختلافات في سلوك الصحفيين بناء على مدى فهمهم للأمن الرقمي؛ فالصحفيون ذوو العقلية الأمنية المتقدمة أكثر وعيًا بكيفية حماية أنفسهم رقميًا، وقادرون على العمل والتواصل بأمان مع الزملاء ومع المصادر، كما يسعون إلى تثقيف أنفسهم من خلال التعلم المستمر عن الأدوات والتقنيات التي يمكنهم استخدامها من أجل تعزيز الحماية الرقمية؛ ليس فقط من أجل التحرر من المراقبة، ولكن أيضًا من أجل حرية إنتاج أنواع محددة من القصص الصحفية الحساسة، التي تتطلب القدرة على التواصل بشكل آمن.

وسعت دراسة حول الوعي بالأمن الرقمي وممارسات الصحفيين (Çalışkan B., 2019)[31] إلى قياس وعي الصحفيين، الذين يستخدمون التكنولوجيا الرقمية، بالأمن الرقمي، والتعرف على التدريب الأمني الرقمي الذي يتلقونه، وذهبت النتائج إلى أن الصحفيين في تركيا يعتمدون بشدة على التكنولوجيا الرقمية، ويعتبرونها أداة أساسية في البحث عن القصص الصحفية، أو كتابتها، أو توزيعها، خاصة فيما يتعلق بالاعتماد على البريد الإلكتروني ووسائل التواصل الاجتماعي؛ إلا أنهم يفتقرون إلى المعرفة بالأدوات التي تجعل اتصالاتهم الرقمية أكثر أمنًا، فعلى سبيل المثال، رغم أن لديهم مستوى عامًا من الوعي بمخاطر هجوم التصيد الاحتيالي، التي

تشكلها روابط الويب، ورسائل مواقع التواصل الاجتماعي، ومرفقات البريد الإلكتروني مجهولة المصدر، فإنه تم التقليل من أهمية إجراءات الأمان عند التعامل مع خدمات البريد الإلكتروني أو التدوين.

وتناولت ورقة بحثية لـ(Lokman T., 2019)[32] أهمية الأمن الرقمي، باعتبارها ضمانة لحرية الصحافة؛ حيث ترى أن وصف حرية الصحافة يتعلق بالقيود المفروضة عليها وبالتهديدات الخارجية، وتقدم توصية للباحثين في مجال الصحافة بالاهتمام بالتكنولوجيا الحديثة، ورفع الوعي بممارسات الأمن الرقمي، باعتباره أحد التحديات الرئيسية لحرية الصحافة، فهي تفترض أن عدم وعي الصحفيين بالممارسات الأمنية السليمة، يجعلهم يحدون من العمل على الموضوعات الصحفية الشائكة، مما يعني حتمية الحاجة لرفع الوعي بالأمن الرقمي قبل الشروع في كتابة الموضوعات الصحفية الحساسة، بعد تزايد الرقابة الرقمية ضد الصحفيين.

وأظهرت الدراسة التي أجريت حول الأمن الرقمي بين الصحفيين النيجيريين (Olunifesi S. and Olawale O., 2017)[33] أن لدى الصحفيين مستوى إدراك جيدًا، حول التهديدات التي تواجههم، التي كان من أهمها تعرض الحسابات للخطر، وحملات التضليل والتشويه الإلكترونية، وهجمات المواقع الزائفة، إلا أنهم لا يمتلكون بعد المهارات الخاصة بالأمن الرقمي المطلوبة للعمل في البيئة الرقمية؛ حيث اتسمت إجراءات الأمن التي يقومون بها بالبساطة؛ مثل تغيير كلمة المرور، واستخدام مضاد الفيروسات وجدار الحماية، وقد أظهروا مواقف إيجابية نحو الحاجة للتدريب على الأمن الرقمي، لمعالجة الفجوة المعرفية الملحوظة، وإعطاء الأولوية لإعدادات الأمان لحساباتهم على وسائل التواصل الاجتماعي والأجهزة الرقمية.

وفي أحد المسوح التي أجريت لقياس كيف يستفيد الصحفيون حول العالم من التكنولوجيا لتعزيز أمنهم (Javier R., 2016)[34]، استجاب فيه 154 صحفيًا من دول مختلفة على مستوى العالم، مثل (الولايات المتحدة الأمريكية وأمريكا اللاتينية وأوروبا والشرق الأوسط وآسيا وإفريقيا)، حصلت رغبة الصحفيين في حماية الاتصالات عبر الإنترنت؛ مثل البريد الإلكتروني أو

الدردشة، على أعلى معدلات الاستجابات بين الصحفيين، وكان مستوى الوعي نحو حماية الاتصالات بين الصحفيين في أمريكا الشمالية وأوروبا أعلى من الصحفيين في الدول الأخرى، بينما كان الوعي تجاه سبل حماية الملفات مرتفعًا لدى الصحفيين من كافة الدول، ومن أعلى إستراتيجيات الحماية من وجهة نظر الصحفيين تخزين الملفات ومشاركتها مع زملائهم، بينما كان تشفير الأجهزة، مثل أجهزة الكمبيوتر والأجهزة اللوحية والهواتف الذكية، أقل شيوعًا.

وترى دراسة (McGregor and Watkins, 2016)[35] أن الطريقة التي يفكر بها معظم الصحفيين حول الأمن الرقمي يمكن وصفها بأنها "الأمان من خلال الغموض"، حيث إن الاعتقاد السائد لدى الصحفيين أنهم لا يحتاجون إلى اتخاذ احتياطات أمنية معينة، ما لم يشاركوا في عمل حساس بدرجة كافية لجذب الانتباه إليهم، أو في حال كانت الموضوعات الصحفية التي يغطونها ذات أهمية للجهات الفاعلة، أو تتعلق بالأمن القومي؛ وتوضح الدراسة أن هذا الاعتقاد يعد غير مناسب؛ نظرا للمخاطر الأمنية الفعلية التي يواجهها الصحفيون بصفة عامة، حتى أولئك الذين يغطون الموضوعات المحلية أو الاجتماعية، حيث إن احتمال تعرض الفرد لمخاطر أمنية، على الأرجح، يكون بسبب عمله كصحفي، مما يجعله هدفًا محتملا، وعلى الرغم من التهديدات واسعة النطاق، والمخاطر الرقمية الملموسة، فإن الصحفيين لم يفعلوا الكثير لتغيير ممارساتهم في مجال أمن المعلومات أو الاتصالات في السنوات الأخيرة، وتشير النتائج إلى أن ذلك على الأرجح بسبب سوء فهم أنظمة الاتصالات التكنولوجية.

وتظهر نتائج دراسة عن الأمن الرقمي للصحفيين الاستقصائيين بأمريكا (Mitchell A., et al., 2015)[36] أن حوالي ثلثي الصحفيين يعتقدون أنهم عرضة للمراقبة والقرصنة الإلكترونية، وأن الحكومة الأمريكية ربما قامت بجمع بيانات حول مكالماتهم الهاتفية، أو رسائل البريد الإلكتروني الخاص بهم، وأن هذه المخاوف كانت سببًا في توقفهم عن متابعة بعض التحقيقات أو محاولة الوصول إلى مصادر بعينها، حيث يعتقدون أيضا أن كونهم صحفيين يزيد

من احتمال جمع بياناتهم، لذلك ازدادت رغبتهم في تغيير سلوكهم الرقمي، مثل الطريقة التي يخزنون بها، أو يشاركون فيها، مستندات هامة، أو الطرق التي يتواصلون فيها مع المصادر، ورغم ذلك، يؤكد الغالبية العظمى منهم أن فوائد الاتصالات الرقمية تفوق المخاطر.

وأظهرت نتائج بحث أجرته مؤسسة فريدم هاوس والمركز الدولي للصحفيين (Sierra J., 2013)[37] حول الأمن الرقمي للصحفيين والمدونين المكسيكيين؛ أنه على الرغم من اعتمادهم الكبير على الإنترنت والشبكات الاجتماعية ومنصات التدوين، وزيادة استخدام الهواتف المحمولة واعتبارها الأكثر اعتمادا لدى الصحفيين لجمع المعلومات، فإنهم يعانون قصورًا في مستوى استخدام أدوات الحماية الرقمية؛ مثل التشفير، واستخدام الشبكات الافتراضية الخاصة VPNs، وحذف الملفات بشكل آمن، وأفاد المبحوثون أن أبرز المخاطر الرقمية التي يواجهونها هي التجسس الإلكتروني، وأقروا جميعهم تقريبا (96% منهم) أنهم يعرفون زملاء لهم تعرضوا لهجوم إلكتروني، كما أفادوا بأنهم لا يتمتعون بالكفاءة الكافية لاستخدام أدوات الأمان الرقمية.

وفي دراسة (Franziska R., et al. 2015)[38] حول ممارسات الأمن الرقمي للصحفيين واحتياجاتهم؛ استهدفت المقاربة بين الصحافة، وبين مجالات الأمن الرقمي؛ لتطوير أدوات اتصال آمنة للصحافة، باعتبار أن الصحفيين مستخدمون محتملون للاتصالات الآمنة وأدوات تخزين البيانات، وذهبت النتائج إلى الاعتماد المحدود على أدوات الأمان الحالية؛ بسبب تحديات خاصة بقابلية الاستخدام، وعدم التوافق بين الممارسات والأولويات من جهة، وبين القيود المفروضة على الصحفيين من جهة أخرى؛ رغم ما أكده المبحوثون من تعرضهم لمخاطر مباشرة؛ مثل التنصت وسرقة البيانات وتلقي التهديدات وسرقة أجهزة الحاسوب الخاصة بهم. ومن بين تقنيات تخزين الملفات يلاحظ زيادة الاعتماد على طرق التخزين السحابية، على الرغم من المخاطر الأمنية للتخزين السحابي، التي قد تتمثل في تعريض البيانات لطرف آخر، (وقد عبر عدد قليل من المبحوثين عن هذا القلق)؛ لذلك تعتبر الدراسة أن الممارسات الصحفية الآمنة يجب أن تعتمد على تعاون

حقيقي بين أمن الكمبيوتر والاتصالات الرقمية، وبين مجتمع الصحافة.

وأشارت دراسة حول احتياجات الناشطين الرقميين في فيتنام (SecondMuse, 2014)[39] إلى تفاوت إدراك الصحفيين لإستراتيجيات الأمن الرقمي، فعلى سبيل المثال، هناك عدم إدراك لدى معظم الصحفيين والمدونين لماهية التشفير، ومن كان لديه علم بالبريد المشفر لم يحاول استخدامه، بينما لديهم الوعي حول أمان كلمة المرور؛ حيث يقومون بتغيير كلمات المرور الخاصة بهم بانتظام، واستخدام كلمات مرور أكثر تعقيدًا، بالإضافة إلى ارتفاع الوعي باستخدام المصادقة الثنائية، واستخدام أدوات مكافحة البرامج الضارة ومضادات الفيروسات.

وناقشت دراسة لمركز الأخبار للابتكار والتعليم (Internews Center, 2012)[40] الأمن الرقمي للصحفيين في باكستان، وفق محاور الاستخدامات التكنولوجية في العمل الصحفي، والمخاطر الرقمية المحتملة ووعي الصحفيين بها، بالإضافة إلى البحث عن إستراتيجيات الأمن الرقمي التي ينتهجونها، وذهبت النتائج إلى محدودية الوعي بالأمن الرقمي لدى الصحفيين؛ حيث إن غالبيتهم يعتقدون أن الأمن الرقمي يعني فقط الحفاظ على أجهزة الكمبيوتر الخاصة بهم آمنة من فيروسات الإنترنت، والذي يمكن تحقيقه ببساطة عن طريق استخدام لبرنامج جيد لمكافحة الفيروسات، وأشار 90% منهم إلى أنهم لم يتلقوا أي تدريب على كيفية ضمان أمنهم الرقمي.

المحور الثاني: إرشادات الأمن الرقمي للصحفيين، والاتصالات الآمنة:

دفع الاهتمام بتوعية الصحفيين إزاء المخاوف المتعلقة بالرقابة الإلكترونية إلى تقييم المخاطر، ووضع عدة إرشادات حول أفضل الممارسات الأمنية الرقمية، سواء من قبل مؤسسات أو منظمات مختلفة، أو من قبل بعض الباحثين، فقدمت دراسة (Michelle F. and Nisha G., 2018)[41] لبعض أنواع الإساءات والمخاطر التي قد يتعرض لها الصحفي، وقدمت مجموعة من الإرشادات والتدابير الأمنية للحماية الرقمية؛ لضمان سلامتهم

على الإنترنت، كما قدمت توصيفًا لمنصة ''ترول بسترز TrollBusters''، باعتبارها منصة متخصصة في مناهضة العنف الإلكتروني للصحفيين، وأشارت أيضًا إلى توفر دروس في الأمن الرقمي للصحفيين.

وأشارت دراسة (Ron D., 2017)[42]، حول الهجمات الرقمية وكيفية مواجهة تحدياتها وقيمة الأساليب المتبعة في تعزيز الأمن، إلى أن أدوات الاتصالات الآمنة ضرورية، وقد تساعد في الحماية من التهديدات الرقمية؛ إلا أنها غير كافية؛ حيث إن أي تشفير، حتى وإن كان متطورًا، فإنه لن يحصن الصحفي ضد المخاطر، حيث فتحت قضية سنودن نافذة على المدى الهائل الذي تتعرض فيه الاتصالات الرقمية لخطر المراقبة من قبل الحكومات؛ وقدمت نموذجًا حول كيفية القيام بالتجسس؛ لذا فإنه من المحتمل أن تتوسع المخاطر المحيطة بالوسائط الرقمية الخاصة بالصحفيين على المدى القريب.

لا قصص بدون مصادر.. ومن أجل أن تكون الممارسات الأمنية الصحفية قوية وفعالة، يجب أن يتم توفير الحماية الحقيقية للمصادر؛ لذلك قدمت دراسة (Susan M., 2015)[43] إرشادات للأمن الرقمي وحماية مصادر الصحفيين، ومنها: تشفير البيانات، والإخفاء الرقمي للمعلومات، وحذف الملفات غير الضرورية بطريقة آمنة، وطرق تصفح الويب واستخدام البريد الإلكتروني والدردشة والرسائل النصية والمكالمات الصوتية بوسائل آمنة.

وتأكيدًا على أهمية أمن المعلومات للصحفيين، قدم كل من (Carlo S. and Arjen K., 2014)[44] دليلا عمليًا هامًا لضمانات وإجراءات تسهم في حماية وأمن الصحفيين، خاصة الاستقصائيين، ومصادرهم، حيث يشرح كيفية التواصل عن طريق الكتابة بأمان؛ سواء عبر البريد الإلكتروني، أو الرسائل القصيرة، أو برامج وتطبيقات الدردشة، وكيفية تلقي وتخزين وإرسال المعلومات، وكيفية اختيار أنظمة الحاسوب، وطرق التصفح بأمان، واختيار كلمات مرور قوية، كما قدمت (شبكة إنترنيوز Internews)[45] منهجًا تدريبيًا للأمن الرقمي، بمثابة دليل للمدربين، يشمل: طرق تقييم المخاطر، كيفية الحماية من البرامج الضارة، الحفاظ

على سلامة البيانات، البحث عبر الإنترنت بأمان، حماية البريد الإلكتروني، نصائح لحماية الهاتف الذكي وجهاز الكمبيوتر.

وأصدر (مجلس البحوث والتبادلات الدولية IREX)[46] منهجًا تدريبيًا للعاملين في مجال الإعلام، والعاملين في مجال التواصل الاجتماعي، احتوى مجموعة من المحاور؛ منها السلامة البدنية، ومحور دروس نفسية واجتماعية، بالإضافة إلى دروس حول الأمن الرقمي، تهتم بالفجوة الرقمية، والهندسة الاجتماعية، وتأمين كلمات المرور، والحفاظ على أجهزة الكمبيوتر آمنة، وأمن المتصفحات، وأمن الهواتف الذكية.

وقدمت (اليونسكو) دليلا حول الأسباب التي تجعل من الصعوبة تحديد الهجمات والتهديدات التي تواجه الصحفيين، حيث ترى أن تحديد الهجمات الرقمية يحتاج إلى مستوى عال من الخبرة الرقمية، فعلى الرغم من أن بعض المؤسسات الإخبارية قد يكون لديها موارد تساعدها في تحديد هذه التهديدات، فإن العديد من الصحفيين المستقلين ليس لديهم هذه الخبرات، ولا الفرص في رفع مستوى معرفتهم الرقمية، وقدمت بهذا الدليل نماذج للتهديدات والتحديات، وأيضا التوصيات[47].

وأوضح (Micah L., 2013)[48] توجيهات حول كيفية حماية الخصوصية والمصادر في عصر مراقبة الأمن القومي، حيث عرض أنواع التشفير المختلفة وجدواها، ونماذج التهديد التي ينبغي إدراكها بصورة جيدة، قبل التفكير في معرفة كيفية استخدام أدوات التشفير؛ حيث إن تحديد ما هو مستهدف يمكّن الصحفي من حمايته، ومن أهم الإرشادات التي قدمها كيفية إدارة كلمات المرور، والمصادقة الثنائية، وتشفير القرص الصلب والمكالمات والنصوص، وإخفاء الهوية باستخدام متصفح Tor، وبين ما لا يحميه هذا النوع من المتصفحات، وعادات التصفح، والدردشة خارج السجل أي غير المحفوظة Off-the-Record (OTR)، بالإضافة إلى التعريف بالبيانات الوصفية الخاصة بهذا النوع من المحادثات وطرق ضمان المجهولية.

أما فيما يتعلق بالاتصالات الآمنة فيوجد قدر كبير من العمل القائم في مجالات الاتصالات الآمنة وتخزين البيانات بأمان، على سبيل المثال تهدف

عديد من تطبيقات الهواتف الذكية إلى توفير الرسائل النصية الآمنة، أو الاتصالات الآمنة، مثل تطبيق ويكر Wickr[49] لتشفير المحادثات وحذفها تلقائيًا، وتطبيق سيجنال Signal[50]، ومشروع الجارديان Guardian Project[51] للتطبيقات الآمنة، الذي يقدم تطويرًا لبرمجيات وتطبيقات من أجل حماية الاتصالات والبيانات الشخصية من التطفل والاعتراض والمراقبة، وتوفر مجموعة من تطبيقات سطح المكتب إمكان تشفير القرص الصلب، مثل سي كلينر CCleaner[52]، وتروكربت TrueCrypt[53]، بالإضافة إلى أنظمة الأمان التي تهدف إلى توفير تصفح مجهول على الإنترنت، عبر برنامج تور Tor[54]، ويهدف تايلز Tails[55] إلى توفير نظام تخفٍّ خاص، يركز بشكل كبير على الخصوصية، كما أن هناك العديد من الأدوات التي تقدم تشفيرًا لرسائل البريد الإلكتروني والدردشة، مثل بي جي بي Pretty Good Privacy (PGP)، وكريبتوكات CryptoCat، وحاول العديد من مزودي خدمة البريد الإلكتروني أيضا تقديم بريد إلكتروني آمن ومجهول، مثل سايلنت سيركل Silent Circle، ولافابيت Lavabit، وعلى الرغم من أن جميع هذه الأدوات، وما يماثلها، تعد أدوات ذات قيمة؛ فإن لديها بعض نقاط الضعف؛ إذ يفتقر البريد الإلكتروني المجهول ''لافابيت Lavabit''، على سبيل المثال، إلى الحماية القانونية، حيث أثيرت إشكاليات حول الخصوصية المطلقة، وإن كان الموقع يوفرها بالفعل، خاصة بعد أن شهد إقبالا كبيرًا في أعقاب قضية سنودن، الذي كان مستخدمًا لهذه الخدمة، وهو ما جعل الحكومة الأمريكية تستجوب مالك الخدمة، وطالبته بتقديم المعلومات الخاصة بعمل الخدمة، مما قد يعرض خصوصية المستخدمين للخطر، الأمر الذي جعله يعلن عن إيقاف الخدمة بسبب تحقيق حكومي، على حد تصريحه، ومن أهم ما قاله: (إذا كنت تعرف ما أعرفه عن البريد الإلكتروني فقد لا تستخدمه)[56]، كما أثارت مجموعة من التساؤلات حول خدمة تشفير اتصالات الهواتف الذكية Silent Circle مخاوف حول الخصوصية، حيث بادرت الشركة بإغلاق خدمة البريد الإلكتروني الخاصة بها، موضحين ''أنهم يستبِقون الحكومة الأمريكية قبل إجبارهم على تقديم

بيانات العملاء"، بينما أبدوا ثقتهم في أنهم يستطيعون حماية الرسائل النصية والمكالمات الصوتية ومكالمات الفيديو، إلا أن البريد الإلكتروني كان دائمًا أقل أمانًا؛ كونه يعتمد على بروتوكولات الإنترنت[57].

وتعد شبكة Tor، وفقًا لما ورد في دراسة (Norcie G., et al., 2014)[58]، واحدة من أكثر شبكات إخفاء الهوية استخدامًا في العالم، إلا أن هناك بعض التحديات الخاصة بقابلية الاستخدام، حيث تفترض إحدى الدراسات أن قابلية استخدام برنامج الأمان من قبل المستخدمين تتطلب أن يكون المستخدم على دراية بالمهام التي يحتاج إلى القيام بها بكفاءة، دون ارتكاب أخطاء، وبتكلفة مناسبة.

إلا أن بعض مواقع المؤسسات تحاول توفير إجراءات أمنية عالية، تضمن خصوصيتها وسريتها، مثل قاعدة بيانات المركز السوري للعدالة والمساءلة (SJAC)، الذي يقوم بتوثيق وتحليل انتهاكات قانون حقوق الإنسان والقانون الجنائي الدولي؛ من خلال مشاركة الأفراد للبيانات الوصفية والمعلومات، من قبيل المكان والزمان وأدوات الانتهاك، حيث تخضع هذه القاعدة لبروتوكولات أمان وقواعد صارمة خاصة بمشاركة البيانات مع أي طرف، وذلك من أجل حماية موثقي وجامعي البيانات[59].

وترى نتائج دراسة (Shirley G. and others, 2006)[60] أنه على الرغم من وجود فائدة للبريد الإلكتروني المشفر لحماية الرسائل؛ فإنها تفترض أن السياق الاجتماعي هو الذي يكون وراء قرارات المستخدمين بشأن ما إذا كان سيتم تشفير البريد الإلكتروني أو لا، ومتى يتم ذلك، حيث يعتبر البعض أن تشفير البريد الإلكتروني مثل الشعور بـ(بجنون العظمة)، وأن تشفير الرسائل ليس لكونها سرية، وليس لارتباطها بعامل سهولة الاستخدام، ولكن بسبب عوامل اجتماعية.

المحور الثالث: النماذج الذهنية للأمن الرقمي:

استخدم العديد من دراسات أمن الحاسوب النموذج الذهني، كمدخل نظري لها، منها: دراسة (Emilee R. and Rick W., 2015)[61] حول شيوع المصادر غير الرسمية للحصول على معلومات متعلقة بأمن الكمبيوتر،

حيث إن قليلا من الأشخاص يتلقون تدريبات صريحة على أمن الكمبيوتر، مما يؤثر في قدرتهم على اتخاذ قرارات أمنية جيدة، ودراسة حول تأثيرات النماذج الذهنية على أمن الكمبيوتر لـ(Emilee R. and Rick W., 2011)[62]، من أجل فهم كيفية تشكيل النماذج الذهنية لمستخدمي الكمبيوتر غير التقنيين، ودراسة حول النماذج العقلية لمخاطر أمن الحاسوب (Farzaneh A. et al., 2007)[63]، لمعرفة النماذج الذهنية للخبراء وغير الخبراء فيما يتعلق بمجموعة من المخاطر الأمنية، ودراسة ''النماذج الشعبية'' كنموذج عقلي لأمن الكمبيوتر المنزلي، (و''الشعبية'' تشير إلى الأفراد العاديين الذين ليسوا خبراء ولم يتلقوا تدريبا)، وذهبت دراسة (Rick W., 2010)[64] إلى أنه على الرغم من صناعة الأمان الكبيرة التي توفر البرامج اللازمة للحماية، فإن مستخدمي الكمبيوتر المنزلي لم يمثل عنصر الأمن في تطبيقاتهم الفعلية وجودًا حقيقيًا، مما يعرضهم لخطر الاختراق، وتحدد الدراسة عدة نماذج للمخاطر الأمنية من أجل تحديد أدوات الأمن التي يجب استخدامها.

وأجريت دراسة حول النموذج الذهني للإنترنت والآثار المترتبة على الخصوصية والأمن (Ruogu K. et al., 2015)[65]، حيث تقسم النماذج الذهنية للمستخدمين إلى (نماذج بسيطة ونماذج مفصلة)، هذا الاختلاف بين تصورات المستخدمين منشؤه الخلفيات التعليمية، حيث كان لدى المستخدمين الذين ليس لديهم خلفية تعليمية عن علوم الكمبيوتر نماذج عقلية بسيطة، بينما كان لدى أولئك الذين يحظون بخلفية مرتبطة بعلوم الكمبيوتر نموذج مفصل حول المعلومات الخاصة بكيفية عمل الإنترنت؛ وكان لديهم وعي أكبر حول من الذي يمكنه الوصول إلى بيانات المستخدمين واتصالاتهم عبر الإنترنت، إلا أن هذه الخلفية التقنية لم ترتبط بسلوك مباشر أكثر أمانا في تعاملهم على الإنترنت.

دراسة (Priya K. et al., 2017) حول النماذج الذهنية للأطفال والخصوصية والأمن عبر الإنترنت[66]، ودراسة (Cristian B. et al., 2010)[67] حول النماذج العقلية لتحذيرات أمن الكمبيوتر التي تهدف إلى حماية المستخدمين وأجهزة الكمبيوتر الخاصة بهم، والتي ترى أن هذه التحذيرات قد تكون غير

ذات جدوى في بعض الأحيان، بسبب تجاهلها بصورة متكررة، ودراسة حول تصورات المستخدمين للمخاطر والأضرار على الويب (Batya F., et al., 2002)[68]، حيث توصلت الدراسة إلى أن غالبية المشتركين اعتمدوا على علامات مرئية لتحديد معيار الاتصالات الآمنة، مثل وجود HTTPS وأيقونة القفل.

وفي إطار تشكيل النماذج الذهنية عبر وسائط إعلامية، سعت دراسة (Fulton et. al., 2019)[69] إلى معرفة ما إذا كانت القصص التي يتم سردها في القصص الخيالية بالتليفزيون والسينما تؤثر على معرفة المستخدمين بالأمن الرقمي أو لا؛ وكيف تؤثر هذه المعرفة على التصورات الذهنية لأمن الكمبيوتر، والسلوك الأمني المترتب على ذلك، ووجدت الدراسة أن النماذج الذهنية تتأثر بالمعلومات المقدمة من خلال الإعلام، وأن بعضها يلعب دورًا في اتخاذ المستخدمين قرارات أمنية، وبعض هذه الاعتقادات كانت سلبية، مثل اعتقاد المستخدمين أن القرصنة والمخاطر الأمنية أمر لا مفر منه، وأن المستخدمين العاديين ليسوا مهمين بما يكفي لجذب انتباه المتسللين الرقميين، وبعضها كان إيجابيًا حيث تمثل في زيادة الوعي بخطر الخداع ورسائل البريد الإلكتروني المشبوهة.

واهتمت بعض الدراسات بالمصدر الذي يعتمد عليه المستخدمون للحصول على نصائح للأمن الرقمي، مثل دراسة (Elissa M. et al., 2016)[70]، التي ذهبت نتائجها إلى وجود عدة مصادر أساسية يعتمد عليها المستخدمون الذين يتعاملون مع بيانات حساسة، منها: المتخصصون في تكنولوجيا المعلومات، ومكان عملهم، والخبرات من الأحداث السلبية؛ سواء تم التعرض لها شخصيًا، أو معرفتها من قبل الأحداث الدائرة؛ ويحدد المستخدمون إذا ما كانوا سيقبلون نصيحة الأمان الرقمي، بناء على مصداقية مصدر المشورة، وقد يرفض المستخدمون بعض النصائح لأسباب عديدة؛ منها الاعتقاد بأن بعض النصائح قد تحتوي على الكثير من المواد التسويقية أو تهدد خصوصيتهم، ودراسات أخرى ترى أن بائعي البرامج وخدمات تكنولوجيا المعلومات ومواقع الويب والأصدقاء والحكومات ووسائل الإعلام

أحد المصادر المحتملة للمعلومات المتعلقة بالأمن، مثل: (Steven F and Liam M, 2014)[71]، ودراسة (Tabitha J., et al., 2013)[72].

بينما ركزت دراسات أقل على النوايا والسلوكيات المتعلقة بأمن مستخدمي الكمبيوتر على الوعي والمعرفة كشرط وضرورة، ولكن ليس كافيًا، لاتخاذ قرارات أمنية مناسبة لحماية أجهزتهم، بمعنى آخر يحتاج الأشخاص إلى معرفة شيء ما حول التهديدات وكيفية التقليل من حدتها، من أجل اتخاذ قرارات جيدة متعلقة بالأمان، مثل دراسة (Furnell S., 2007)[73] ، ودراسة (Robert L., et al., 2008)[74].

من العرض السابق للدراسات السابقة يمكن استخلاص المؤشرات التالية:

1. في الوقت الذي تهتم فيه الدولة بقطاع الأمن السيبراني، وتأكيدها على ضرورة توعية الأفراد، ودعمها لإستراتيجية قومية وطنية للأمن الرقمي، إلا أن هناك مبادرات عدة أفرزت مجموعة من الأدلة التوجيهية العامة، كما سبقت الإشارة إليه في مقدمة الدراسة، لكنها ليست دراسات أكاديمية، ولم تجد الباحثة، حتى الانتهاء من إجراء الدراسة، دراسات أكاديمية عربية تتناول الأمن الرقمي للصحفيين.

2. تعتبر الدراسات التي تناولت الأمن الرقمي للصحفيين، على وجه التحديد، دراسات وصفية اهتمت بوصف طبيعة الاستخدامات والمخاطر والتهديدات، إلا أنها لم تعتمد إلى إطار نظري، ويظهر الاستثناءان الوحيدان في دراسة (McGregor and Watkins, 2016)، ودراسة (Tsui L., and Francis L., 2019)، حيث اعتمدت كل منهما على النموذج العقلي، كمحاولة لتفسير تصورات الصحفيين للأمن الرقمي.

3. أشارت الدراسات السابقة إلى تزايد اعتماد الصحفيين على الأجهزة والأدوات الرقمية، وزيادة الاعتماد على الأجهزة المحمولة والإنترنت والشبكات الاجتماعية ومنصات التدوين، مع زيادة المخاطر الرقمية التي قد يتعرضون لها، مثل الرقابة الإلكترونية، وسرقة البيانات، والقرصنة الرقمية؛ مما يستلزم معه التعرف على إدراك الصحفيين لأدوات تعزيز الأمن الرقمي.

4. أظهرت الدراسات أن الصحفيين لا يمتلكون المعرفة الكافية بمهارات السلامة الرقمية، رغم أنهم أظهروا مواقف إيجابية نحو إدراكهم للتهديدات التي يواجهونها فيما يتعلق بسلامتهم الرقمية، لذلك فهم بحاجة إلى توفير تدريب مناسب لمعالجة فجوة المعرفة، التي يمكن ملاحظتها بين إدراكهم للمخاطر، وعدم قدرتهم على العمل بأمان.

5. أشارت نتائج الدراسات إلى وجود تفاوت في مستوى الوعي بالأمن الرقمي لدى الصحفيين، حيث يزداد الوعي لدى الصحفيين بأمريكا الشمالية وأوروبا عن الدول الأخرى، فيما يتعلق بحماية الاتصالات، أما الوعي تجاه حماية الملفات فكانت مرتفعة لدى الصحفيين من عدة دول؛ وتسعى الدراسة الحالية إلى الوقوف على توصيف الوعي بالأمن الرقمي لدى الصحفيين المصريين.

6. تدلل النتائج على انخفاض مستوى استخدام أدوات الحماية الرقمية القوية، مثل التشفير، واستخدام الشبكات الافتراضية الخاصة، وذلك بسبب صعوبة القابلية للاستخدام.

7. أشارت نتائج الدراسات أيضا إلى أن استخدام أدوات الأمن الرقمي الأكثر تطورا محدودة للغاية، في مواجهة التهديدات الحقيقية التي قد يخشى منها الصحفي، وأوصت هذه الدراسات بضرورة رفع مستوى تعليم وتدريب الصحفيين على الأمن الرقمي.

8. ركزت بعض الدراسات على ارتباط الوعي بالتهديدات، كحافز للبحث عن الأمن واتخاذ قرارات أمنية، إلا أنها لم تتطرق إلى مصادر هذا الوعي، وتحاول هذه الدراسة تحديد دور المؤسسات الصحفية كمصدر لدعم الوعي الرقمي للصحفيين.

9. كما يتضح من النتائج أيضا أن التدريب الأمني ليس جزءًا من مهام أغلب المؤسسات الصحفية، لكنها ثقافة خاصة ومجهود ذاتي للصحفي.

تساؤلات الدراسة:

- ما الاستخدامات الرقمية للصحفيين؟ وما اتجاهاتهم نحو مشكلات الأمن الرقمي؟
- إلى أي مدى يدرك الصحفيون المصريون التهديدات الرقمية المحتملة؟
- ما هو دور المؤسسات الصحفية في تدعيم مفهوم الأمن الرقمي لدى الصحفيين؟
- ما مستوى معرفة الصحفيين بالأدوات التي تعزز الأمن الرقمي؟
- ما مستوى استخدامات الصحفيين الفعلية لأدوات تعزيز الأمن الرقمي؟
- ما التحديات التي يواجهها الصحفيون والتي قد تقف عائقا أمام ممارسة أمنية جيدة؟

فروض الدراسة:

- توجد علاقة بين مستويات معرفة الصحفيين بالأساليب والأدوات الخاصة بالأمن الرقمي، وبين مستويات استخدامهم الفعلي لها.
- توجد علاقة بين مستوى معرفة الصحفيين بالتهديدات الرقمية المحتملة، وبين الإستراتيجيات الفعلية التي ينتهجونها لتطبيق أدوات الأمن.
- توجد فروق بين المبحوثين الذين تعرضوا لمخاطر رقمية والذين لم يتعرضوا لها وبين مستوى استخدامهم لأدوات الأمن الرقمي.
- توجد فروق بين استخدام المبحوثين لأدوات الأمن الرقمي وفقا لمستوى الخبرة الرقمية لديهم.

الإجراءات المنهجية للدراسة:

منهج الدراسة وأداتها:

تعتمد الدراسة على منهج المسح، وداخل إطار هذا المنهج تم الاعتماد على منهج المسح بالعينة، واعتمدت الدراسة على صحيفة الاستقصاء الميدانية، كأداة لجمع البيانات التي تقيس متغيرات الدراسة، في ضوء المشكلة البحثية والأهداف والتساؤلات والفروض، وتوزعت أسئلة الاستقصاء على خمسة

محاور أساسية، تضم بعض المقاييس على النحو التالي:

المحور الأول: استخدام الصحفيين للأجهزة الرقمية المختلفة، ورؤيتهم لطبيعة المشكلات التي تتعلق بالأمن الرقمي، وإذا ما كانت التكنولوجيا غيرت الطريقة التي يدير بها الصحفيون عملهم.

المحور الثاني: تصوراتهم حول التهديدات الأمنية الرقمية وأنواع الاختراقات المختلفة، والأهداف التي يخشى الصحفيون أن تمثل تهديدًا لأمنهم الرقمي.

المحور الثالث: دور المؤسسات الصحفية في تدعيم مفهوم الأمن الرقمي لدى الصحفيين واحتياجاتهم التدريبية.

المحور الرابع: مقياس معرفة الصحفيين لأدوات الأمن الرقمي.

حيث تم بناء هذا المقياس من 18 عبارة، حيث قدرت الإجابات: نعم=3، محايد=2، معارض=1، وبالتالي فإن محصلة هذا المقياس تتكون من (37) درجة، من 17 : 54، تم تقسيمها إلى ثلاثة مستويات؛ مستوى منخفض (18 : 30)، مستوى متوسط (31 : 42)، ومستوى مرتفع (43 : 54).

المحور الخامس: مقياس استخدام الصحفيين الفعلي لأدوات الأمن الرقمي.

حيث تم بناء هذا المقياس من 23 عبارة، حيث قدرت الإجابات: نعم=3، محايد=2، معارض=1، وبالتالي فإن محصلة هذا المقياس تتكون من (47) درجة، من 23 : 69، تم تقسيمها إلى ثلاثة مستويات؛ مستوى منخفض (23 : 38)، مستوى متوسط (39 : 54)، ومستوى مرتفع (55 : 69).

المحور السادس: مقياس التحديات التي يرى الصحفيون أنها قد تقف عقبة أمام أمنهم الرقمي.

تم بناء هذا المقياس من 12 عبارة، حيث قدرت الإجابات: نعم=1، محايد=0، معارض=(-1)، وبالتالي فإن محصلة هذا المقياس تتكون من (25) درجة، من (-12) : 12، تم تقسيمها إلى ثلاثة مستويات؛ مستوى منخفض (-12 : -4)، مستوى متوسط (-3 : 3)، ومستوى مرتفع (4 : 12).

مجتمع الدراسة واختيار العينة:

تم تحديد مجتمع الدراسة في الصحفيين العاملين بالمؤسسات الصحفية المصرية، مع مراعاة تمثيل كافة أنماط الملكية في العينة، حيث تم اختيار الصحفيين من مؤسسات أخبار اليوم، اليوم السابع، الوطن، الشروق، الوفد، وتم تطبيق الدراسة في الفترة من يناير 2020 حتى مارس 2020؛ على عينة متاحة قوامها (180) مفردة، كان عدد الاستمارات الصالحة للاستخدام (137).

توصيف خصائص العينة:

المتغير	المجموعات	ك	%
الفئة العمرية	(من 21 سنة إلى أقل من 30 سنة)	59	43.1%
	(من 30 سنة إلى أقل من 40 سنة)	58	42.3%
	(من40 سنة إلى أقل من 50 سنة)	16	11.7%
	50 سنة فأكثر	4	2.9%
	الإجمالي	137	100%
النوع	ذكر	87	63.5%
	أنثى	50	36.5%
	الإجمالي	137	100%
طبيعة الإصدار الإعلامي الذي تعمل به	صحيفة مطبوعة	77	56.2%
	موقع إلكتروني	60	43.8%
	الإجمالي	137	100%
نمط ملكية الصحفية	خاصة	86	62.8%
	قومية	33	24.1%
	حزبية	18	13.1%
	الإجمالي	137	100%

توزيع العينة على الصحف	اليوم السابع	37	27%
	أخبار اليوم	33	24.1%
	الوطن	33	24.1%
	الوفد	18	13.1%
	الشروق	16	11.7%
	الإجمالي	137	100%
عدد سنوات الخبرة في المجال الصحفي	أقل من 5 سنوات	35	25.5%
	من 5 سنوات : 10 سنوات	61	44.5%
	أكثر من 10 سنوات : أقل من 20 سنة	36	26.3%
	أكثر من 20 سنة	5	3.6%
	الإجمالي	137	100%
المستوى التعليمي	مؤهل عال	132	96.4%
	حاصل على درجة الماجستير أو الدكتوراه	5	3.6%
	الإجمالي	137	100%
الخبرة التقنية	مبتدئ	50	36.5%
	متوسط	76	55.5%
	مرتفع	11	8%
	الإجمالي	137	100%

اختبارا الصدق والثبات:

تم التأكد من صدق استمارة الاستقصاء، وأنها تقيس ما ينبغي قياسه، وأن الأسئلة تعكس أهداف الدراسة، وتساؤلاتها، حيث تم قياس صدق الاستمارة من خلال عرضها على مجموعة من المحكمين[75] للتحقق من مصداقيتها وشمولها، وأنها تقيس بالفعل ما استهدفته الدراسة، وفي ضوء ملاحظاتهم تم تعديل الاستمارة حتى وصلت إلى شكلها النهائي الصالح للتطبيق.

أما ثبات صحيفة الاستقصاء فقد تم تطبيق إعادة الاختبار على 20 مفردة، وذلك بعد 15 يومًا من تطبيق الاستمارة للمرة الأولى، وكانت نسبة الارتباط بين إجابات المبحوثين في المرتين 0.91، وهي نسبة تدل على دقة البيانات ووضوح الاستمارة، كما تم حساب معامل الثبات ألفا كرونباخ لمقاييس الدراسة، والتي تراوحت نسبتها (0.710 كحد أدنى إلى 0.897 كحد أعلى)، وهي نسبة ثبات مقبولة، تجعل تطبيق المقياس ممكنًا.

المعالجة الإحصائية للبيانات:

تمت معالجة البيانات إحصائياً باستخدام الحاسب الآلي، وذلك باستخدام برنامج SPSS؛ لملاءمته لطبيعة الدراسة، وإمكانية تكوين جداول تكرارية بسيطة، وجداول تكرارية توضح العلاقات الارتباطية بين المتغيرات، حيث تم استخدام الوسط الحسابي، الانحراف المعياري، كما تم حساب كا2، ومعامل التوافق لمعرفة الفروق بين متوسطات درجات العينة على مقاييس الدراسة.

مفهوم الأمن الرقمي:

تُستخدم مصطلحات (Digital Security أو Cyber Security)، للدلالة على الأمن الرقمي أو الأمن السيبراني، ويحدد الاتحاد الدولي للاتصالات الأمن السيبراني بأنه مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات والمبادئ ومناهج إدارة المخاطر والتدريبات والإجراءات وأفضل الممارسات والضمانات التكنولوجية، التي من الممكن استخدامها لحماية المستخدم والمنظمات بصورة عامة[76].

ويعرف الأمن الرقمي بأنه ممارسة المستخدمين نشاطًا للدفاع عن الأصول التكنولوجية من محاولات الخصوم للتدخل في تلك الأصول، ويمكن أن يتخذ الدفاع أشكالا متعددة، منها الاستجابة بشكل مباشر للهجمات بالتصدي لها، أو البحث الاستباقي بمعرفة الاتجاهات الدفاعية عبر محاولة توقع تصرفات المهاجمين، أو تحديد الإجراءات التي يجب اتخاذها عند معرفة ثغرة أمنية لم يتم استغلالها بعد[77]، أو هو مجموعة تدابير مصممة لحماية أجهزة وأنظمة الكمبيوتر من الوصول أو الهجوم غير المصرح به[78]، أو

ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة[79]، حيث يقصد بالهجمات الرقمية المحاولات المستمر للتسلل إلى الأجهزة والشبكات والبنى التحتية للأفراد أو المجموعات أو المنظمات[80].

كما يعرف بأنه مجموعة من الأدوات والسياسات، ومفاهيم الأمن، والضمانات الأمنية، والمبادئ التوجيهية، وأساليب إدارة المخاطر، التي يمكن استخدامها لحماية البيئة الرقمية والمستخدمين وأصول المستخدمين؛ مثل الأجهزة والبنى التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات المرسلة أو المخزنة في البيئة الإلكترونية، بحيث تشمل أهداف الأمان العامة: الإتاحة، والنزاهة، والسرية، ويتجاوز الأمن الرقمي مفهوم أمن المعلومات Information Security؛ حيث يبحث في حماية العامل البشري كأهداف محتملة للهجمات السيبرانية[81]، وعادة ما تسمى حماية البيانات التي يتم إنشاؤها وتخزينها ونقلها بين أجهزة الحوسبة بالأمن الرقمي، أو الأمن السيبراني؛ فهي حالة حماية من الاستخدام غير المصرح به، أو غير المقصود للبيانات، ويُطلق خبراء الأمن الرقمي على الأشخاص أو الأجهزة المستخدمة لاعتراض البيانات اسم ''الجهات الفاعلة السيئة''، التي تستهدف ''الأصول'' ذات القيمة، التي يمكن تخزينها وتبادلها بين الأجهزة الرقمية[82].

وتعرّف الباحثة الأمن الرقمي إجرائيًا، في إطار هذا البحث، بأنه آلية أو سلسلة من الإجراءات التي يقوم بها الصحفي لحمايته، عبر منع أو تأخير وقوع هجمات سيبرانية، تستهدف أصوله (خصوصيته وبياناته وأجهزته).

أهمية الأمن الرقمي:

أصبح الأمن الرقمي مسألة ذات أهمية عالمية، فقد نشرت أكثر من 50 دولة إستراتيجية تحدد موقفها الرسمي من الفضاء الإلكتروني والجريمة الإلكترونية والأمن الرقمي، وتدرج بريطانيا الأمن السيبراني كأولوية قصوى، حيث خصصت نحو 650 مليون جنيه إسترليني، على مدى أربع سنوات،

لبرنامج الأمن الرقمي، وتنفق الحكومة الأمريكية 19 مليار دولار على الأمن السيبراني[83]، وفي مصر نصت المادة 31 من الدستور المصري، يناير 2014، على أن ''أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون''، وأطلق المجلس الأعلى للأمن السيبراني المصري، التابع لرئاسة مجلس الوزراء، ''الإستراتيجية الوطنية للأمن السيبراني'' 2017-2021، التي تهدف إلى تأمين البنى التحتية للاتصالات والمعلومات[84]، كما أصدر الاتحاد الدولي للاتصالات دليلا للأمن السيبراني للبلدان النامية.

وفي مجال الإعلام، ومع ما يسمى ''الهاكتيفزم Hacktivism''، أي استخدام القرصنة لتعزيز أجندة سياسية، ظهرت هجمات القرصنة السياسية ضد المؤسسات الإعلامية أو خدمتها، كما هو الحال في وثائق بنما، لذلك أصبح الأمن الرقمي مصدر قلق كبير للمؤسسات الإعلامية؛ سواء ما يتعلق باختراق مواقع الويب والتطبيقات الإعلامية والإخبارية، أو سرقة الهوية، مما جعل إجراءات الحصول على الأمن الرقمي مشكلة حقيقية ومكلفة، بالنسبة للمؤسسات الإعلامية، لم يكن معظمها مستعدًا بشكل كاف للتعامل معها، خاصة في عصر الحوسبة السحابية، مثل الهجمات الإلكترونية المتكررة على مؤسسات إعلامية كبرى؛ مثل نيويورك تايمز وواشنطن بوست ووكالة أسيوشيتدبرس[85]، وكانت أبرز القضايا محاكمات التسريب التي اعتمدت على البيانات الوصفية للاتصالات الرقمية والهجمات التقنية على المؤسسات الإخبارية، وتم الإبلاغ عن هجمات تقنية متطورة من قبل دول قومية، مثل الصين وكوريا الشمالية، إلا أن الهجمات الأكثر شيوعًا، والتي أصبحت أيضا أكثر تكرارًا، هي هجمات التصيد الاحتيالي phishing attacks، وهجمات الاستغلال exploitation attacks[86].

وفي مصر، شهدت مواقع بعض الصحف، مثل المصري اليوم واليوم السابع، عددًا من الهجمات الإلكترونية، حيث استهدفت قرصنة الموقع من أجل دس محتوى خبري، عبر مجموعة من الأخبار المفبركة، بالإضافة إلى اختراق

خدمة الرسائل الإخبارية القصيرة لجريدة الوطن.

وهناك العديد من التهديدات التي تجعل الصحفيين في احتياج إلى الأمن الرقمي، والنظر في استثمار بعض الأدوات الأمنية، ولعل من أهمها **جرائم الإنترنت**، التي تشمل استهداف الأنظمة الخاصة بالمؤسسة، أو الأفراد، من أجل تحقيق مكاسب مالية، أو التسبب بحدوث خلل بالأنظمة، **والهجمات السيبرانية** التي غالبا ما تنطوي على جمع معلومات ذات دوافع سياسية[87].

جميع هذه التهديدات تعد سببًا يجعل مساعي المؤسسات تتجه نحو الاهتمام بتعزيز الأمن الرقمي، وقد أثارت قضية سنودن مسألة الأمن الرقمي لدى الصحفيين، وأصبحت قضايا المراقبة والأمن السيبراني من القضايا الأساسية على الساحة الصحفية، ولعبت أدوات التشفير دورًا أساسيًا في تسهيل التواصل بين المصدر والصحفيين، وألهم النقاش حول التشفير، الذي أعقب قضية سنودن، الصحفيين والمؤسسات الإعلامية لتبني إستراتيجيات وممارسات الأمن الرقمي، من أجل حماية عملهم بشكل أفضل، في عصر المراقبة الرقمية، التي أصبحت منتشرة، وفي الوقت ذاته، تضاعفت حالات تأثر الصحافة بالقرصنة، التي تمثلت في التسريبات مثل (أوراق بنما، والتسريبات السويسرية، وتسريبات لوكسمبرج)[88].

التحديات التي تطرحها بعض تطبيقات ومنصات الاتصال:

تطرح الأشكال الرقمية الحديثة لمنصات الاتصال وتطبيقاته تحديات جديدة، تزيد من تهديد خصوصية الأفراد، مثل الحوسبة السحابية، والشبكات الاجتماعية، والهواتف الذكية، ومحركات البحث.

فالهاتف المحمول، أدى منذ ظهوره إلى إثارة بعض القضايا المتعلقة بالخصوصية، مقارنة بالاتصالات الهاتفية للخطوط الثابتة، حيث أثارت ميزة معرفات الجهاز المحمول IMEI وبطاقة SIM المخاوف تجاه القدرة على تحديد الموقع الجغرافي للجهاز المحمول، وقدرة أطراف ثالثة على اعتراض الاتصالات، وتزايدت هذه المخاوف اليوم مع دمج مزايا الإنترنت مع الهواتف، لتتشكل الهواتف الذكية، مما أدى إلى تنامي مخاوف انتهاك الخصوصية، نظرًا لزيادة

مستوى الشخصنة في هذه الوسيلة، وارتفاع مستوى بيانات المستخدم عليه، وتسهم هذه الأجهزة، على نطاق آخر، في زيادة الأطراف الثالثة التي يمكنها الوصول إلى بيانات المستخدم، مثل (مزود خدمة الإنترنت عبر الهاتف المحمول، الشركة المصنعة للجهاز، مزود نظام التشغيل، مطوري التطبيقات المستخدمة عليه)[89]، ولا تزال الهواتف الذكية تمثل حالة من التحول السريع والابتكار في تقديم إمكانات جديدة، بما في ذلك القياسات الحيوية، مثل مسح بصمة الإصبع، وبصمة الوجه، واستخدام الإيماءات للتحكم في الأجهزة، ثم التطور الذي أحدثه ارتباط الأجهزة الذكية القابلة للارتداء بتهديد الخصوصية[90].

أما الحوسبة السحابية، وهو مصطلح يشير إلى تخزين كميات متزايدة من البيانات في ''سحابة'' عبر الإنترنت، مما يشكل خطرًا على السيطرة الشخصية على تلك البيانات، فبمجرد أن يتم تخزين البيانات في السحابة يمكن على سبيل المثال نقل معلومات المستخدم من مزود إلى مزود، أو من جهاز لآخر، كما يؤدي تغيير سياسات الخصوصية وشروط الاستخدام إلى مزيد من المخاطر، خاصة وفي بعض الأحيان لا يكون الأفراد مدركين للآثار المترتبة على هذه التغييرات[91]، لذلك أصبح حتميًا على مقدمي الخدمات السحابية توفير درجة عالية من الشفافية لمستخدميهم، فمن المهم معرفة من قام بإنشاء البيانات، ومن قام بتعديلها، وإذا كانت بيانات المصدر يمكن استخدامها لأغراض التتبع والتدقيق والتحكم في الوصول إلى الملفات[92].

وتبدو تأثيرات الأمان على الشبكات الاجتماعية أكبر من مثيلتها من التهديدات السابقة، فيما يتعلق بالخصوصية، حيث تعتمد هذه الشبكات أيضا على نموذج أعمال قائم على الإعلانات، أكثر تعقيدًا من محركات البحث، حيث تعتمد الشبكات الاجتماعية على المحتوى الذي ينتجه ويساهم به المستخدمون، والذي يعد في مجمله معلومات شخصية وبيانات خاصة دقيقة، تمثل مفتاح العملية للشبكات الاجتماعية، أما محركات البحث، التي يتمثل دورها تاريخيًا في وظيفة مهمة، وهي المساعدة على تصفح الموارد الهائلة المتاحة على الإنترنت، والتي تقدم هذه الخدمة بشكل

مجاني مع نموذج أعمال يعتمد على الإعلان؛ حيث لا يدفع المستخدمون أموالا، ولكن من خلال إتاحتهم لبياناتهم يتم تخصيص الإعلانات على أساس هذه البيانات، لضمان أعلى نسبة مشاهدة وتفاعل، لذلك كلما كانت البيانات الشخصية محددة بدقة، كانت أفضل وأكثر اكتمالا لتحقيق الهدف، لذلك توسعت محركات البحث نحو تقديم خدمات أشمل، مثل البريد الإلكتروني، أو مشاركة الصور، أو السحابة، أو تحرير المستندات. ورغم ما تتيحه هذه الخدمات من سهولة وتكامل للمستخدم، فإنها تمكن هذه المحركات من إنشاء ملفات تعريف متكاملة للمستخدمين[93].

المخاطر والتهديدات الرقمية:

تعد البيانات التي يقدمها الأفراد في العالم الافتراضي متاحة، ليس فقط لأنفسهم، إنما تتم إتاحتها وجمعها وتخزينها بطريقة مركزية، بواسطة شركات الإنترنت؛ مثل جوجل أو آبل أو فيسبوك، وفي كثير من الأحيان لا يعرف الأشخاص ما هي البيانات التي يتم جمعها وتخزينها؛ وقد تتبادل الشركات بيانات الأفراد بين بعضها البعض، كما يمكن أن يتم التحكم بهذه البيانات بواسطة كيانات أخرى لها اهتمامات مختلفة أحيانا عن اهتمامات الفرد[94]، لذلك يعد حصول الآخرين (الأطراف الثالثة)؛ سواء كانوا شركات أو أفرادًا أو هيئات، على البيانات الوصفية من أكثر أشكال التهديدات شيوعًا.

كما يعد التتبع الجغرافي من أبرز المخاطر، حيث يمكن تتبع مكان تواجدك؛ سواء عبر الهاتف أو عبر جهاز الكمبيوتر، ما دام التتبع الجغرافي مُفعلا وقيد التشغيل على جهازك، والبرامج الضارة أيضا؛ فقد يحتوي الهاتف أو جهاز الكمبيوتر على برنامج لا تعرفه، مما يمنح الأطراف الأخرى إمكانية الوصول إليه، ومحاولات القرصنة، والانتحال عبر الشبكة، والمراقبة؛ سواء من قبل الحكومات أو الشركات أو الأفراد المتتبعين[95]، وقد تطورت البرمجيات الخبيثة من شكلها التقليدي؛ (فيروسات، ديدان الكمبيوتر Worms، أحصنة طروادة Trojans)، إلى أشكال جديدة أكثر تطورًا وتعقيدًا، حيث تستهدف الثغرات الأمنية في الأنظمة[96].

وإذا نظرنا إلى التهديدات الرقمية المحتملة، من منظور ما يجب علينا حمايته، فإنه يمكن تناول هذه التهديدات عبر عنصرين أساسيين؛ (الهوية والبيانات)، والهوية قد تكون الخاصة بك، أو هويات الذين تتواصل أو تتعامل معهم، أما البيانات فهي كل نص أو صورة أو فيديو أو جدول بيانات أو أي شيء يمكن نقله إلكترونيًا؛ مما يجعل حماية كل من الهوية والبيانات أمرًا ضروريًا، يجب إعطاؤه الأولوية لتشفير قوي[97]، وعلى المستوى الصحفي أصبح الصحفيون اليوم أكثر عرضة للخطر، ليس فقط أثناء قيامهم بالمهام في الأماكن الخطرة، ولكن أيضا في حياتهم اليومية، أو في غرفة الأخبار، أو في الطريق في ظل زيادة المراقبة الرقمية؛ فكما سهل العالم الرقمي مهنة الصحافة فإنه أيضا جعلها أكثر خطورة، وفي الوقت ذاته يمكن أن تقدم التكنولوجيا الرقمية أدوات لتقليل المخاطر التي ينبغي على الصحفيين البحث عنها واستغلالها[98].

فتمكّن الإنترنت اليوم من جمع أنواع جديدة من المعلومات الشخصية، التي تخلق قدرات للجهات المختلفة لتحليل المعلومات الشخصية، مما يسهم في خلق فرص جديدة للاستخدام التجاري للبيانات[99]، حيث تعني زيادة القدرة الحاسوبية أن كميات هائلة من المعلومات، بمجرد جمعها، يمكن تخزينها وتحليلها وربطها بقواعد بيانات، مما يزيد من احتمال انتهاك الخصوصية، فكل نقرة إلكترونية تحدث تسجيلا في مستودع بيانات، وتبقى بانتظار أن يتم استخراجها للتعرف على سلوكنا، فجميع أجهزتنا اللوحية وأجهزة الهاتف والكمبيوتر تقوم بالإبلاغ عن كل صفحة ويب نقوم بزيارتها، وكافة الارتباطات التي نتحرك من خلالها، كل التفاعلات التي تتم عبر البريد الإلكتروني، أو الرسائل الفورية، أو مواقع التواصل الاجتماعي، أو الصور الفوتوغرافية التي تحمل علامات الهوية أو الموسومة جغرافيًا[100].

وتتجاور الخصوصية مع مجهولية الهوية معًا في مجال الاتصالات الرقمية، حيث تزداد مخاطر التهديدات الأمنية؛ سواء للأفراد أو للمنظمات أو للحكومات على حد سواء، فإلى جانب التهديدات المعروفة التي تشكلها الفيروسات الرقمية المختلفة تأتي أشكال الخداع الأخرى، مثل التصيد الاحتيالي أو

التتبع، في مقدمة المخاطر الأمنية، ويؤدي غياب الوعي بهذه التهديدات إلى انتهاكات تؤثر على الأفراد والمنظمات، فمع كل نقرة إلكترونية يتم رسم مسارات رقمية للأفراد يمكن تجميعها وتحليلها؛ وإلى جانب المساس بهوية الأشخاص تقدم أدوات التشبيك الاجتماعي فرصًا لتقليل الحماية التي يمكن توفيرها، فتتسع معها الآثار الرقمية للأفراد[101]، وعلى عكس آثار الأقدام على الرمال غالبًا ما تستمر مسارات البيانات عبر الإنترنت بعد فترة طويلة، ومع ازدياد ارتياح مستخدمي الإنترنت لفكرة نشر المحتوى، أصبحوا أيضًا أكثر وعيًا بالمعلومات التي تبقى مرتبطة باسمهم عبر الإنترنت[102]، ويعد هذا الوعي هو المرحلة الأولى من انتهاجهم مجموعة من التدابير والإستراتيجيات للتقليل من هذه الآثار، أو الحفاظ على الأثر الإيجابي، الذي يقدم صورة إيجابية عنهم، ويحسن من سمعتهم الرقمية.

أدوات الصحفيين للأمن الرقمي ودور المؤسسات الصحفية في تعزيز الأمن الرقمي:

يقسم البعض الأمن الرقمي إلى أمن الشبكة، بمعنى حمايتها من المتسللين؛ سواء كانوا مهاجمين مستهدفين أو برامج ضارة، وأمن التطبيقات؛ حيث يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، وأمن المعلومات وخصوصية البيانات؛ سواء في التخزين أو النقل، وأمن التشغيل، أي العمليات الخاصة بمعالجة أصول البيانات وحمايتها، مثل أذونات المستخدمين عند الوصول إلى الشبكة، وتخزين البيانات أو مشاركتها، والتعافي من الكوارث واستمرارية العمل؛ بمعنى مدى استجابة المؤسسات لحادث الأمن الذي يتسبب في فقد العمليات أو البيانات، وعودة عمل النظام بنفس السعة التشغيلية قبل الحادث الأمني، وتثقيف المستخدم؛ مثل تعليمه حذف المرفقات المشبوهة، وعدم توصيل محركات أقراص مجهولة الهوية[103].

لا يحتاج كل صحفي إلى جميع أساليب وأدوات الأمن الرقمي، ولكن ينبغي أن يكون لديه، على الأقل، فهم أساسي لما يمكن أن تقدمه هذه الأساليب،

وكيفية تطبيقها عند الضرورة، مثل تشفير البيانات، والاتصالات المشفرة من طرف إلى طرف (سواء البريد الإلكتروني أو الدردشة أو المؤتمرات عن بعد)، وحذف البيانات الوصفية، وإنشاء نسخ احتياطية آمنة على التخزين السحابي أو الأقراص، والتصفح الخاص، وحذف سجلات التصفح وملف تعريف الارتباط، واستخدام VPN لإخفاء حركة المرور على الإنترنت، وإدارة كلمات المرور[104].

وهناك عدة مصادر يمكن أن تسهم في رفع وعي الصحفيين بالأمن الرقمي، مثل الموضوعات المتخصصة المنشورة بوسائل الإعلام المختلفة، وصفحات الويب المتخصصة التي تقوم عليها جهات خارجية، والتجارب الشخصية التي يرويها الأفراد، وتشير إحدى الدراسات إلى أن مواقع الويب المتخصصة هي الأكثر موثوقية بالنسبة للمستخدمين، حيث الاعتقاد بأن القائمين على هذه المواقع متخصصون ومحترفون، على عكس التجارب الشخصية التي تميل إلى الكشف عما يهتم به غير المحترفين، وما الذي اختبروه، وعكس ما تقدمه المقالات الإخبارية في وسائل الإعلام، حيث تقوم بالتركيز على القضايا ذات الصلة بمجتمع أكبر، وليس مجتمع الصحفيين خاصة، وليس هناك شك في أن التدريب المتخصص داخل المؤسسات الصحفية نفسها سوف يكون له بالغ الأثر في الفائدة، حيث إن برامج التثقيف الأمني والتوعية تميل إلى أن تكون تحفيزية ومقنعة، أكثر من أن تكون واقعية [105].

ورغم أن البعض يرون أن مسئولية توعية الصحفيين بالأمن الرقمي تقع على عاتق المؤسسات الصحفية، فإن بعض الصحفيين يعملون بشكل حر، أو يعملون في منظمات ناشئة، ليس لديها الدعم المالي الكافي، مما يجعل الحاجة إلى مساهمة المنظمات المهنية العامة، والجهات الفاعلة المختصة بدعم الصحفيين، في توفير التوجيهات حول الأدوات اللازمة للحماية[106]، وتعد حاجة المؤسسات الإعلامية للأمن الرقمي ضرورية للمؤسسة نفسها، خاصة مع تحول المنصات الإعلامية إلى الإنترنت؛ سواء عبر المواقع أو الشبكات الاجتماعية أو التطبيقات.

نتائج الدراسة ومناقشتها:

أولا: الاستخدامات الرقمية للصحفيين:

جدول رقم (1) يوضح مستوى اعتماد المبحوثين على الأجهزة الرقمية عند جمع الأخبار ونشرها

الأجهزة الرقمية	الإجمالي	
	ك	%
الهاتف الذكي	96	70.1%
لابتوب	54	39.4%
جهاز الحاسوب	43	31.4%
تابلت	15	10.9%
الإجمالي	ن= 137	

تشير نتائج الجدول السابق رقم (1) إلى شيوع استخدام الهاتف الذكي من قبل المبحوثين في العمل الصحفي، حيث بلغت النسبة (70.1 %) لاستخدام الهاتف الذكي، يليها استخدام اللابتوب بنسبة (39.4 %)، ثم استخدام جهاز الحاسوب بنسبة (31.4 %)، ثم التابلت بنسبة (10.9 %)، ويلاحظ أن النسبة الإجمالية تتخطى حجم العينة؛ نظرًا لإتاحة الخيار للصحفيين لاختيار أكثر من وسيلة.

تدلل هذه النتائج على شيوع الأجهزة الحديثة، متمثلة في الهاتف الذكي، نظرًا لسهولة حمله، وتعدد إمكاناته، التي يمكن أن تجعله جهازًا يعتمد عليه، خاصة في المواقف الطارئة، والأحداث التي تحتاج إلى سرعة أداء، دون الحاجة للانتظار للحصول على أجهزة مناسبة، مثل كاميرا التصوير أو جهاز الحاسوب لكتابة الموضوعات، وتفق هذه النتيجة مع دراسة (Çalışkan B., 2019)، ودراسة (Internews Center, 2012)، كما تتفق مع دراسة (Sierra J., 2013)، حيث زيادة الاعتماد على التكنولوجيا الرقمية، واستخدام الهواتف الذكية، واعتبارها أداة أساسية في البحث عن القصص الصحفية أو كتابتها أو توزيعها.

جدول رقم (2) يوضح طرق تخزين المبحوثين للبيانات

طرق تخزين البيانات	الإجمالي	
	ك	%
تخزين سحابي مثل: (Dropbox ، Yandex Drive ، Google Drive ، OneDrive)	54	39.4%
تخزين تلقائي على القرص الصلب بالكمبيوتر	50	36.5%
محركات أقراص فلاش (USB)	16	11.7%
أجهزة تسجيل الصوت والفيديو	10	7.3%
أقراص تخزين صلبة خارجية External	7	5.1%
الإجمالي	137	100%

تشير نتائج الجدول السابق رقم (2) إلى ارتفاع نسبة الاعتماد على التخزين السحابي من قبل المبحوثين، بنسبة (39.4 %)، يليه التخزين التلقائي على القرص الصلب بأجهزة الكمبيوتر (36.5 %)، ثم الاعتماد على محركات أقراص فلاش (USB) بنسبة (11.7 %)، يليه الاعتماد على أجهزة تسجيل الصوت بنسبة (7.3 %)، ثم الاعتماد على أقراص التخزين الصلبة الخارجية بنسبة (5.1 %).

ويتضح من هذه النتائج ارتفاع الاعتماد على التخزين السحابي، ويقصد بالتخزين السحابي نموذج للتخزين معتمد على (السحابة)، أي الإنترنت، في حفظ الملفات، بدلا من حفظها على أقراص التخزين بالكمبيوتر، أو الوسائل المادية الأخرى للتخزين، حيث تقدم مواقع عديدة خدمة التخزين، وتفيد أيضا في إتاحة وصول الفرد لملفاته عبر الإنترنت، مما يجعلها جاهزة بصورة دائمة في حال الاحتياج إليها، دون الحاجة إلى ضرورة الوصول إلى الأجهزة التي تم تخزين الملفات عليها، كما تتميز أيضا بإمكان مشاركتها مع آخرين عبر رابط، ومزامنة الملفات التي يتم العمل عليها عبر الجهاز بشكل تلقائي في التخزين السحابي، دون الحاجة إلى إعادة حفظ الملف

على السحابة، وعلى الرغم من المزايا العديدة التي يوفرها الاعتماد على التخزين السحابي فإنه يشير إلى ارتفاع نسبة المخاطر الأمنية الرقمية، التي يمكن أن تواجه الصحفيين، حيث إن التخزين السحابي تكتنفه مجموعة من المخاطر، أهمها فقدان البيانات، والذي يمكن أن يحدث لأسباب عدة، مثل تعرض موقع الخدمة السحابية للاختراق، أو فقدان البيانات، أو السطو على الحسابات، أو الثغرات التكنولوجية نتيجة إتاحة البيانات عبر وسيط اتصالي للتخزين، مما يعني انتقال سيطرة الفرد على ملفاته إلى هذه المواقع، التي بدورها أيضا قد تتعرض للاختراق، مما يعرض بيانات وملفات الفرد للاختراق بالتبعية؛ وغير ذلك من مخاطر، مما يستلزم ضرورة القيام بمجموعة من الإجراءات التي تساعد على رفع درجة الأمان للبيانات المخزنة على هذا النحو.

كما يعد ارتفاع الاعتماد على التخزين التلقائي على القرص الصلب بأجهزة الكمبيوتر، وهي طريقة التخزين التقليدية لمن يعمل على جهاز الحاسوب؛ انعكاسًا لنتيجة الجدول رقم (1) الخاصة باستخدامات الصحفيين لأجهزة الحاسوب، سواء لابتوب أو جهاز الحاسوب المكتبي.

وينخفض الاعتماد على طرق التخزين الأخرى مثل محركات أقراص فلاش (USB)، أجهزة تسجيل الصوت والفيديو، أقراص تخزين صلبة خارجية External، حيث تعتبر USB وسيلة شائعة لحفظ الملفات بصورة مؤقتة لنقلها من جهاز إلى آخر؛ حيث يمكن أن تتعرض لمخاطر فقدان البيانات بصورة سريعة، سواء من خلال فقدانها، أو تلف الملفات عليها، مما يجعل استخدامها كوسيلة حفظ أمرًا محفوفًا بالمخاطر، لذلك لا يشيع استخدامها، كما يمكن أن تتعرض أقراص التخزين الخارجية أيضا لنفس المخاطر، بينما تعد الأجهزة الخاصة بحفظ الصوت والفيديو؛ سواء كاميرا أو آيبود أو جهاز تسجيل، في طريقها للانتهاء، بعد إتاحة كل هذه الخواص وأكثر في أجهزة الهاتف الذكي.

تتفق هذه النتائج مع نتائج دراسة (Franziska Roesner, et al. 2015)، حيث يلاحظ زيادة الاعتماد على طرق التخزين السحابية.

جدول رقم (3) يوضح طرق تواصل المبحوثين مع المصادر أو الزملاء

طرق التواصل	الإجمالي	
	ك	%
الهاتف	91	66.4%
تطبيقات الرسائل الفورية مثل Whatsapp – viber	86	62.8%
مواقع التواصل الاجتماعي	63	46%
الرسائل النصية القصيرة SMS	13	9.5%
البريد الإلكتروني	11	8%
ن = 137		

تشير نتائج الجدول السابق (3) إلى أن الهاتف يعد وسيلة التواصل الأكثر شيوعًا للصحفيين مع مصادرهم، بنسبة (66.4 %)، تليها الاعتماد على تطبيقات الرسائل مثل Whatsapp – Viber (62.8 %)، ثم مواقع التواصل الاجتماعي بنسبة (46 %)، ثم الاعتماد على الرسائل SMS بنسبة (9.5 %)، ثم الاعتماد على البريد الإلكتروني (8 %).

ويمكن من هذه النتيجة استخلاص أن الاتصال الهاتفي لا يزال هو الوسيلة الأكثر اعتمادًا للتواصل، يليه مباشرة الاعتماد على تطبيقات التراسل الفوري المجانية المعتمدة على الإنترنت، باعتبارها أداة اتصال قوية، كأداة بديلة عن إرسال الرسائل النصية القصيرة، حيث أصبحت وسيلة شائعة يعتمد عليها الأفراد اليوم في التواصل، خاصة مع توافر الهواتف الذكية المتصلة بالإنترنت، مما يجعل سهولة الوصول للأفراد من خلالها بدون تكلفة، كما تعد القدرة على إرسال الملفات عبرها، ومشاركة الروابط، ميزة هامة في التواصل مع المصدر، وإمداده، أو الحصول على الملفات منه، كما أصبحت كثير من هذه التطبيقات تهتم بتوفير جوانب الأمان في تشفير الرسائل، مما يجعلها ميزة للصحفيين، ويعد اعتماد نسبة كبيرة من الصحفيين على مواقع التواصل

الاجتماعي، كوسيلة للتواصل مع المصادر، انعكاسًا لشيوع الاعتماد على مواقع التواصل الاجتماعي، باعتبارها وسيلة اتصال حديثة، بينما يتراجع اعتماد الصحفيين على البريد الإلكتروني والرسائل النصية القصيرة؛ لتراجع مزاياهما كوسيلتين أمام الوسائل والأدوات السابقة.

جدول رقم (4) يوضح الأدوات الرقمية المستخدمة في تدوين وكتابة الموضوعات الصحفية

الأدوات المستخدمة	الإجمالي	
	ك	%
برامج التحرير النصي على الكمبيوتر	59	43.1%
برامج التحرير والملاحظات على الهاتف	53	38.7%
التسجيل الصوتي	14	10.2%
مواقع التواصل الاجتماعي	11	8%
الإجمالي	137	100%

يشير الجدول رقم (4) إلى الأدوات الرقمية التي يعتمد عليها المبحوثون في تدوين وكتابة الموضوعات الصحفية، حيث تأتي برامج التحرير النصي على الكمبيوتر في الترتيب الأول (43.1 %)، ثم التحرير والملاحظات على الهاتف (38.7 %)، ثم التسجيل الصوتي (10.2 %)، ثم مواقع التواصل الاجتماعي (8 %)؛ مما يشير إلى زيادة الاعتماد على الجانب التقليدي لمستخدمي الكمبيوتر، عبر الاعتماد على برامج التحرير النصي، وزيادة الاعتماد على الشكل الحديث الذي أصبح متداولا، عبر الاعتماد على تطبيقات وبرامج وملاحظات الهاتف في عملية الكتابة والتدوين، بينما لا يعد التسجيل الصوتي أو الكتابة على مواقع التواصل الاجتماعي أدوات فعالة لتدوين الملاحظات وكتابة الموضوعات الصحفية.

جدول رقم (5) يوضح ما إذا كان لدى المبحوثين مشكلات تتعلق بالأمن الرقمي

هل لديك مشكلات تتعلق بالأمن الرقمي؟	الإجمالي	
	ك	%
لا	82	59.9%
نعم	55	40.1%
الإجمالي	137	100%

يشير الجدول رقم (5) إلى أن كثيرًا من المبحوثين لم يكن لديهم اتجاه إيجابي نحو وجود مشكلات تتعلق بالأمان الرقمي، حيث يرى (59.9 %) منهم أنه ليس لديه أي مشكلات أمن رقمي، بينما يرى (40.1 %) أن لديهم مشكلات تتعلق بالأمن الرقمي.

وربما لا تعد هذه النتيجة سلبية تجاه شعور أغلب الصحفيين نحو الأمن الرقمي بصفة عامة، حيث يعتبر الوعي بوجود مشكلة مرتبطًا بالفهم الدقيق لطبيعة أدوات الأمن الرقمي، لذلك فقد يستخدم الصحفيون وسيلة ما بطريقة محددة دون أن تكون لديهم معلومات كافية عن كيفية تعزيز أمنهم الرقمي من خلالها، أو إمكان استخدام وسيلة بديلة توفر أمنًا أكثر، لذلك تعد بيانات هذا الجدول مجرد إشارة مبدئية لاتجاه الصحفيين نحو معرفتهم بوجود مشكلات متعلقة بالأمن الرقمي، والذي سوف يتم قياسه لاحقًا عبر مقياس يوضح اتجاهاتهم نحو عناصر وأدوات الأمن الرقمي.

جدول رقم (6) يوضح رؤية المبحوثين لطبيعة المشكلات التي تتعلق بالأمن الرقمي

رؤية المبحوثين للمشكلات المتعلقة بالأمن الرقمي	الإجمالي	
	ك	%
التشفير الآمن للملفات والدردشة والاتصالات	12	8.8%
تحقيق الأمن في الهواتف الذكية	10	7.3%
تحقيق الأمن والخصوصية في مواقع التواصل الاجتماعي	9	6.6%
التجسس والتتبع الرقمي	8	5.8%
إدارة كلمات المرور	5	3.6%
تأمين جهاز الحاسوب	5	3.6%
الاحتيال الرقمي	4	2.9%
الفيروسات الرقمية	2	1.5%
الإجمالي	ن = 55	

تشير نتائج الجدول رقم (6) إلى أن المبحوثين الذين أشاروا إلى وجود مشكلات تتعلق بأمنهم الرقمي ربطوا هذه المشكلات بـ: التشفير الآمن للملفات والدردشة والاتصالات بنسبة (8.8 %) في الترتيب الأول، ثم كيفية تحقيق الأمن في الهواتف الذكية بنسبة (7.3 %)، يليها تحقيق الأمن والخصوصية في مواقع التواصل الاجتماعي بنسبة (6.6 %)، يليه التجسس والتتبع الرقمي بنسبة (5.8 %)، ثم إدارة كلمات المرور بنسبة (3.6 %)، ثم تأمين جهاز الحاسوب بنسبة (3.6 %)، ثم الاحتيال الرقمي بنسبة(2.9 %)، ثم الفيروسات الرقمية بنسبة (1.5 %).

ويمكن تفسير هذه النتيجة بأن تشفير الملفات والدردشة والاتصالات، باعتبارها الإشكالية الكبرى لدى الصحفيين، يعد انعكاسًا لحساسية مجال العمل الصحفي، ومدى الحاجة إلى الشعور بالأمان، عبر منع الآخرين غير المرغوب فيهم من الاطلاع على محتوى الملفات أو الرسائل والاتصالات،

حيث إن كل ما يمكن تخزينه أو تداوله مع الآخرين عبر الإنترنت يكون معرضًا دائمًا للاختراق من قبل طرف ثالث، كما يعد الاعتماد المتزايد على الهاتف الذكي، والخصوصية الشديدة التي يحفظ من خلالها كل فرد يستخدمه كثيرًا من المعلومات والبيانات الشخصية، تجعل الحاجة إلى فهم إجراءات الأمان على هذه الوسيلة مرتفعة أيضًا، خاصة إذا فقد المستخدم جهازه أو سُرق منه، وبالمثل أيضا الرغبة في تحقيق الأمن والخصوصية على مواقع التواصل الاجتماعي، التي أصبحت وسيلة لجمع البيانات، والبحث عن الأشخاص، وتتبع سلوكهم، وفهم كيفية الحماية أيضا من التجسس والتتبع الرقمي، وربما تأتي مجموعة من المشكلات الخاصة بالأمن، والتي تعتبر تقليدية إلى حد ما، مثل (إدارة كلمات المرور، وتأمين الحاسب والفيروسات الرقمية)، في مرتبة متأخرة، باعتبار أن عامل القلق تجاهها ربما أصبح متداولا إلى حد كبير، ومفهومًا لدى نسبة كبيرة من الأفراد، فأصبح التعامل معه أكثر سهولة عن المشكلات الأخرى.

وتتفق هذه النتائج مع نتائج دراسة (Sierra J., 2013)، حيث أفاد المبحوثون أن أبرز المخاطر الرقمية التي يواجهونها هي التجسس الإلكتروني.

جدول رقم (7): هل غيرت التكنولوجيا الطريقة التي يدير بها المبحوثون عملهم

تغيير طريقة إدارة العمل الصحفي	الإجمالي	
	ك	%
نعم	116	84.7%
لا	21	15.3%
الإجمالي	137	100%

تشير نتائج الجدول رقم (7) إلى أن التكنولوجيا الحديثة غيرت من الطريقة التي يدير بها الصحفيون عملهم؛ حيث أفاد (84.7 %) منهم بذلك،

بينما يرى (15.3 %) منهم أنهم لم يغيروا طريقة عملهم بسبب التكنولوجيا.

يمكن هنا الإشارة إلى أنه أثناء إعداد المخرجة **لورا بويتراس**، لفيلم "**المواطن الرابع**"، الفيلم الوثائقي الذي يدور حول إدوارد سنودن، اعتمدت إجراءات غير اعتيادية، تزيد من الخصوصية، تتمثل في[107]: شراء جهاز حاسوب جديد، واعتماد اختيار الدفع نقدًا حتى لا يتم تتبع موقعها عبر بطاقتها الائتمانية، واستخدمت نظام تشغيل Tails، وهو نظام تشغيل مجاني مصمم بحيث لا يترك أي أثر رقمي على الكمبيوتر، وتحويل جميع البيانات على شبكة Tor، كما اتخذت إجراءات تشفير محركات الأقراص وشبكة Tor ، واعتمدت أيضا على SecureDrop، الذي يسمح للمصادر بمشاركة معلوماتهم مع الصحفيين بطريقة مجهولة، كما أنها تستخدم بالفعل تشفير GPG، والرسائل الفورية المشفرة، وغير ذلك من إجراءات أمنية رقمية؛ وذلك نظرًا لحساسية الموضوع الذي تعمل عليه، مما يمكن أن يعكس تغيير الصحفيين لطريقة عملهم وفقًا لما تتيحه لهم التكنولوجيا الحديثة من خصائص، خاصة عند العمل على موضوعات حساسة، وهو ما يتفق مع رؤية الصحفيين في هذه العينة.

جدول رقم (8) يوضح كيفية تغيير التكنولوجيا الطريقة التي يدير بها المبحوثون عملهم

كيفية تغيير التكنولوجيا لطريقة العمل الصحفي	الإجمالي	
	ك	%
التواصل مع المحررين والمؤسسة الصحفية (أونلاين)	47	40%
الاعتماد على الإنترنت في البحث عن القصص الصحفية	41	35%
التواصل مع المصادر (أونلاين)	18	16%
تخزين ومشاركة الملفات الهامة	10	9%
الإجمالي	116	100%

تشير نتائج الجدول رقم (8) إلى أن أكثر أشكال التغيير، التي أثرت بها التكنولوجيا على عمل الصحفيين، كانت طريقة التواصل بينهم وبين المؤسسة الصحفية، حيث تحولت إلى التواصل (أونلاين)، أفاد ذلك نسبة (40 %) من العينة، يلي ذلك اعتمادهم على الإنترنت في البحث عن القصص الصحفية حيث يرى ذلك نسبة (35 %)، ثم تواصلهم مع المصادر (أونلاين) بنسبة (16 %)، يليها تخزين ومشاركة الملفات الهامة بنسبة (9 %).

ويلاحظ من ذلك الاعتماد على التكنولوجيا في طرق التواصل والبحث عن المعلومات بصورة كبيرة، ويمكن أن يُستنتج من ذلك أن زيادة الاعتماد على الوسائل الرقمية يستلزم معه بالضرورة الانتباه إلى كيفية تحقيق عنصر الأمان عبر هذه الوسائل، فإذا تم الاعتماد عليها كأداة تواصل؛ سواء بين المحررين والمؤسسة الصحفية، أو بين المحررين ومصادرهم، فإن سرية هذه الاتصالات تعد هامة في العمل الصحفي، خاصة لمن يعملون على موضوعات حساسة، وأيضا إذا تم الاعتماد على التكنولوجيا الحديثة والإنترنت في البحث عن القصص الصحفية سوف ينتج عن هذا البحث اتساع في البصمة الرقمية للصحفيين، (البصمة الرقمية هي ما يتركه الفرد خلفه من آثار رقمية نتيجة استخدامه الإنترنت مثل زيارته للمواقع، إعجابه بالصفحات أو انضمامه للمجموعات على مواقع التواصل الاجتماعي .... إلخ)، كما يتطلب تخزين ومشاركة الملفات مع الآخرين تأمين هذه الملفات، وحمايتها من الوصول والاختراق من قبل أطراف غير مرغوب فيهم، أو حتى تلف أو فقدان هذه الملفات.

ثانيا: مستويات معرفة المبحوثين بالتهديدات الرقمية:

جدول رقم (9) يوضح ما إذا كان المبحوث يعتقد أن بياناته على الإنترنت معرضة للاختراق

اعتقاد أن البيانات الشخصية معرضة للاختراق	الإجمالي	
	ك	%
نعم	74	54%
إلى حد ما	57	41.6%
لا	5	4.4%
الإجمالي	137	100%

تشير نتائج الجدول رقم (9) إلى اعتقاد المبحوثين أن بياناتهم الشخصية على الإنترنت قد تكون معرضة للاختراق؛ حيث أفاد ذلك نسبة (54 %) من العينة، بينما يرى (41.6 %) من الصحفيين أن بياناتهم قد تكون معرضة إلى حد ما للاختراق، ونسبة (4.4 %) لا يعتقدون تعرض بياناتهم للاختراق، وقد يكون من الطبيعي، في حالة الاعتقاد بالاختراق، اتخاذ الإجراءات والتدابير الضرورية التي تمنحهم الشعور بالأمن تجاه بياناتهم وعملهم، خاصة مع استهداف الثغرات الأمنية لدى الشركات والمواقع؛ لمحاولة الوصول إلى حسابات المستخدمين.

وتتفق هذه النتيجة مع نتائج دراسة (Olunifesi S. & Olawale O., 2017)، حيث لدى الصحفيين مستوى إدراك جيد حول التهديدات التي تواجههم.

جدول رقم (10) يوضح الجهات التي يعتقد المبحوثون أنها تمثل تهديدًا لأمنهم الرقمي

الجهات التي تمثل تهديدًا للأمن الرقمي	الإجمالي	
	ك	%
التطبيقات التي يتم تثبيتها على الأجهزة والهواتف	54	39.4%
قراصنة الإنترنت	35	25.5%
مزود خدمة الإنترنت	31	22.6%
الشركات التي أشتري منها، أو اشتركت في قوائمها البريدية	29	21.2%
المنظمات الحكومية	28	20.4%
الهواة والمتطفلون	27	19.7%
الشركات التي تمتلك مواقع الويب التي أزورها	27	19.7%
جميع هذه الجهات	19	13.9%
الإجمالي	ن = 137	

تشير نتائج الجدول رقم (10) إلى اعتقاد المبحوثين أن الجهات التي يمكن أن تكون مهتمة بجمع بياناتهم الرقمية، وقد تمثل تهديدًا لأمنهم الرقمي، هي الجهات القائمة على التطبيقات التي يقومون بتثبيتها على أجهزتهم وهواتفهم؛ حيث أفاد ذلك نسبة (39.4 %) من العينة، بينما يرى (25.5 %) من الصحفيين أن قراصنة الإنترنت قد يمثلون التهديد الأكبر فيما يخص جمع بياناتهم الشخصية، بينما يرى (22.6 %) أن هذه الجهات هي مزودو خدمة الإنترنت، ويرى (21.2 %) أن هذه الجهات هي الشركات التي يشترون منها عبر الإنترنت، أو اشتركوا في قوائمها البريدية، بينما يرى (20.4 %) أن المنظمات الحكومية هي التي قد تجمع بياناتهم، ويري (19.7 %) أن الهواة والمتطفلين هم هذه الجهات، بينما يرى (19.7 %) أنها الشركات التي تمتلك مواقع الويب التي يزورها المستخدم، ويرى (13.9 %) من العينة أن جميع هذه الجهات تمثل تهديدًا لأمنهم الرقمي.

ويستخلص من هذه النتيجة اعتبار أن التطبيقات التي يثبتها الصحفيون على أجهزتهم تمثل التهديد الأكبر لأمنهم الرقمي، حيث تتطلب منحها أذونات شاملة من أجل استخدامها، ولا يتحقق كثير من الأفراد من هذه الأذونات، أو يفكرون في عواقبها، أو يقرأون سياسات الخصوصية والاستخدام، والتي قد تمنح قدرًا لا بأس به من البيانات الشخصية، مثل البريد الإلكتروني أو رقم الهاتف، أو التشبيك عبر الحسابات الخاصة بمواقع التواصل الاجتماعي، أو تحديد المكان عبر تطبيقات التعقب وتحديد المواقع، أو رقم بطاقة الائتمان أو العنوان، ويستلزم ذلك وعي الصحفيين بالأذونات اللازمة فقط، والضرورية لعمل هذه التطبيقات، ورفض التطبيقات أو الإعدادات التي تطلب أكثر من ذلك، ومسح التطبيقات غير المستخدمة.

أما القرصنة الرقمية فهي الأنشطة غير القانونية المرتبطة بالتسلل والتلاعب الرقمي، والتي قد تستهدف مجموعة من الجهات الفاعلة مثل الصحفيين[108]، فقراصنة الإنترنت، أو المخترقون، أو ما يسمى بـ(الهاكرز)، تتعدد أساليبهم في جمع البيانات؛ سواء عبر التنصت، أو استدراج المستخدمين إلى برامج تجسس أو فيروسات ضارة؛ (مثل البريد الإلكتروني الشهير، الذي يرسله أحد الأشخاص، ويدعي امتلاكه مبلغًا ماليًا كبيرًا، ويعرض على المستخدم اقتسامه معه، ويطلب رقم حسابه البنكي)، أو استخدام الهندسة الاجتماعية لإقناع الأفراد باحتياجهم لمعرفة محتوى يبدو جذابًا، أو الوصول إلى محتوى مثير، مما يدفع الأفراد إلى محاولة اكتشافه عبر الضغط على روابط، تتيح للمخترق جمع البيانات وكشف المعلومات التي يحتاجها؛ (مثل الاستطلاعات التي على مواقع التواصل الاجتماعي، وألعاب اكتشاف الشخصية ...)، أو اختراق حسابات مواقع التواصل الاجتماعي، هذا بالإضافة إلى قراصنة الإنترنت، الذين يقومون بهجمات إلكترونية، يستهدفون بها المواقع الكبرى، والتي قد تحتوي على بيانات أو ملفات خاصة بالمستخدمين، لذلك فإن اختيار الصحفيين لعنصر قراصنة الإنترنت في الترتيب الثاني يدلل على ارتفاع معرفة ووعي الصحفيين باعتبارهم إحدى الجهات التي تمثل تهديدًا لبياناتهم وأمنهم.

ويمكن إرجاع اختيار المبحوثين لمزود خدمة الإنترنت، باعتباره البوابة التي نستخدم من خلالها الإنترنت، في ترتيب متقدم، إلى وعي الصحفيين بإمكانات مزود الإنترنت بمعرفة كثير من البيانات الخاصة بالأفراد، والتي منها المواقع التي يزورها المستخدم، والكلمات التي يتم البحث عنها ....الخ، كما يدرك المبحوثون أيضا أن المواقع التي يمكن أن يكون قد استخدمها في الشراء الإلكتروني، أو كان قد اشترك في قوائمها البريدية، يمكن أن تحتفظ ببياناته مثل البيانات البنكية أو العنوان أو رقم الهاتف.

بينما تأتي كل من المنظمات الحكومية، والهواة والمتطفلين، والشركات التي تمتلك مواقع الويب التي يزورها المستخدم في ترتيب لاحق، من وجهة نظر الصحفيين.

وتتفق هذه النتيجة مع نتائج دراسة (Ruogu Kang et al., 2015)، حيث يرى المبحوثون أن الشركات التي تستضيف المواقع، والأطراف الثالثة، ومزودي خدمة الإنترنت، والحكومة، من ضمن الجهات التي تستهدف بياناتهم الشخصية، مما يمثل تهديدًا لأمنهم وخصوصيتهم.

جدول رقم (11) يوضح ما إذا كان الصحفي يعتقد أن عمله يزيد من احتمال جمع بياناتهم

احتمال جمع البيانات	الإجمالي	
	ك	%
نعم	131	95.6%
لا	6	4.4%
الإجمالي	137	100%

تشير نتائج الجدول رقم (11) إلى اعتقاد المبحوثين أن عملهم الصحفي يمثل حساسية كبيرة بالنسبة إليهم، قد تجعلهم عرضة لاحتمال جمع البيانات حولهم، حيث أفاد (95.6 %) منهم بذلك، بينما يرى (4.4%) منهم

أن العمل الصحفي لا يزيد من مخاطر احتمال جمع البيانات حولهم.

وتدلل هذه النتيجة على إدراك الصحفيين أن الصحافة، باعتبارها مهنة محفوفة بالمخاطر، لا ترتبط بالمخاطر القانونية أو الجسدية والنفسية؛ ولكن المخاطر الرقمية لها بعد هام أيضا في إدراكهم، وتتفق هذه النتائج مع نتائج دراسة (Mitchell A., et al., 2015)، حيث يعتقد كثير من الصحفيين أنهم عرضة للمراقبة والقرصنة الإلكترونية، وأن هذه المخاوف كانت سببًا في توقفهم عن متابعة بعض التحقيقات أو محاولة الوصول إلى مصادر بعينها.

جدول رقم (12) يوضح المخاطر الرقمية التي يخشى المبحوثون أن تمثل تهديدًا لأمنهم الرقمي

المخاطر المحتملة	الإجمالي	
	ك	%
انتهاك الخصوصية	88	64.2%
الاستيلاء على كلمات المرور الخاصة بي	41	29.9%
الحصول على بيانات الأشخاص الذين أتواصل معهم	32	23.4%
تتبع سلوك الحوسبة الخاص بي	25	18.2%
إصابة الجهاز ببرنامج خبيث يضر بالبيانات	18	13.1%
تتبع تحركاتي عبر معلومات الموقع الجغرافي	18	13.1%
دفعي لزيارة مواقع معينة	15	10.9%
الابتزاز عبر إساءة استخدام المعلومات	10	7.3%
الإجمالي	ن = 137	

تشير نتائج الجدول رقم (12) إلى مجموعة الأهداف التي يعتقد المبحوثون أنها تمثل تهديدًا لأمنهم الرقمي على النحو التالي: انتهاك الخصوصية، حيث يرى ذلك (64.2 %) من العينة، يليها الاستيلاء على كلمات المرور الخاصة بي، بنسبة (29.9 %)، ثم الحصول على بيانات الأشخاص

الذين أتواصل معهم بنسبة (23.4 %)، ثم تتبع سلوك الحوسبة الخاص بي بنسبة (18.2 %)، يليها إصابة الجهاز ببرنامج خبيث يضر بالبيانات بنسبة (13.1 %)، يليها تتبع تحركاتي عبر معلومات الموقع الجغرافي بنسبة (13.1 %)، ثم دفعي لزيارة مواقع معينة بنسبة (10.9 %)، وفي الترتيب الأخير الابتزاز عبر إساءة استخدام المعلومات بنسبة (7.3 %).

ويمكن تفسير هذه النتائج على أن انتهاك الخصوصية الرقمية وتسريب البيانات الشخصية هو الهاجس الأكبر لدى الصحفيين، حيث أصبحت التسريبات الإلكترونية تشكل حروبًا من نوع خاص، قد تكون تجارية من أجل تنفيذ دعايات تسويقية، أو رقابية لتتبع أنشطة الأفراد (على سبيل المثال ما أثير حول أزمة شركة كامبريدج أناليتيكا Cambridge Analytica لتحليل البيانات حيث قامت باستخدام بيانات مستخدمي فيسبوك في أغراض الدعاية السياسية)، وهو الأمر الذي يثير شواغل الأفراد تجاه الحق في الخصوصية الرقمية، والحق في النسيان على الشبكة، كما تدلل النتائج على أن الاستيلاء على كلمات المرور يمثل تهديدًا للأمن الرقمي، خاصة لأولئك الذي لا يختارون كلمات مرور قوية، وهي تأتي في ترتيب متقدم، حيث تعتبر كلمة المرور القوية بمثابة حماية من اختراق الحسابات، حيث عادة ما تكون هجمات الاستيلاء على كلمات المرور مصدرها تحليل لمحاولات سابقة في اختراق الحسابات، مما يسهل الاختراق إذا كانت كلمة المرور ضعيفة، وتعتبر رؤية الصحفيين لأكثر المخاطر أيضا التي قد تمثل تهديدًا لأمنهم الرقمي؛ الحصول على بيانات الأشخاص الذين يتواصل معهم، وهم في الأغلب المصادر الذين يتواصل معهم الصحفي، يعكس وعيه بأهمية حماية مصادره، فعلى الرغم من القوانين تكفل للصحفي الحفاظ على سرية مصادره، فإن التطور التكنولوجي يتيح مراقبة الأفراد مما يجعل الحفاظ على سرية الاتصالات والمصادر محل شك.

كما أشار عدد من المبحوثين إلى مخاطر تتبع سلوك الحوسبة الخاص بهم، والذي أصبح أحد أدوات التقصي، حيث يتضمن هذا السلوك الرسائل والصور التي يتم تحميلها، أو البيانات الوصفية المتعلقة بالوسوم التي يتم النقر

عليها في مواقع الويب؛ فكل اتصال رقمي يحدث حتمًا بصمة رقمية يمكن استخدامها في دراسة خصائص الأفراد والعلاقات الاجتماعية.

وفي ترتيب متأخر يرى المبحوثون أن بعض المخاطر التي تشكل تهديدًا لأمنهم الرقمي تتمثل في إصابة الجهاز ببرنامج خبيث يضر بالبيانات؛ وهي على الرغم من كونها مخاوف ليست حديثة فإنها متزايدة بعد الاعتماد الشديد على الإنترنت، مثل إصابة الأجهزة بفيروسات عبر المواقع الإلكترونية والروابط المختلفة، وتقلل وجهة نظر الصحفيين من مخاوف تتبع تحركاتهم عبر معلومات الموقع الجغرافي المفعل على أجهزة الهاتف على سبيل المثال، ربما نظرا لإمكان تعطيل هذه الميزة مؤقتا، أو إغلاق الهاتف، أو حتى عدم اصطحابه معهم، مما لا يتيح تتبعهم، كما يقل أيضا خطر دفع الصحفيين لزيارة مواقع معينة، ويمكن تفسير ذلك بقدرة الصحفي على تمييز الروابط الضارة والعناوين الزائفة، التي يمكن أن تقوده إلى مواقع غير مرغوب فيها، وتأتي في نهاية هذه المخاطر الابتزاز الإلكتروني عبر التهديد باستخدام بيانات ومعلومات حول الشخص.

ويمكن القول بأنه نظرا لأن الرقمنة في الصحافة وفرت مزايا غير مسبوقة للصحفيين، إلا أنها كشفت أيضًا عن بعض الاتجاهات المثيرة للقلق لديهم، وأصبحت الصعوبات التي يواجهها الصحفيون عبر الإنترنت لا تختلف عن أي تهديدات مادية، فعلى سبيل المثال قد يتعرض موقع الصحيفة أو مدونة الصحفي إلى هجمات حجب الخدمة، مما يؤدي إلى عدم قدرتها على تلبية الطلبات الواردة إليها، نظرًا لحجم المرور الكبير عليه في وقت واحد، أو أن تتم مراقبة حركات الصحفيين عبر بيانات الموقع الجغرافي المرتبطة بالهاتف المحمول، أو أن يتم ربط حياتهم الشخصية عبر البيانات الوصفية لأنشطتهم الخاصة على الإنترنت.

وتتفق هذه النتائج مع نتائج دراسة (Olunifesi S. & Olawale O., 2017) التي ذهبت إلى ارتفاع إدراك الصحفيين نحو المخاطر الرقمية التي يواجهونها، كما تتفق مع نتائج دراسة (Internews Center, 2012)، حيث يرى المبحوثون أن سرقة البيانات وانتهاك الخصوصية من أكثر المخاطر

الشخصية التي يواجهونها، وتتفق أيضًا مع نتائج دراسة (Shere A., et. al. 2020) التي ذهبت إلى أن الصحفيين بشكل عام لا يدركون المخاطر، ولا يحمون أنفسهم بشكل كاف.

جدول رقم (13) يوضح ما إذا كان الصحفي قد واجه أي مخاطر رقمية (أو اختراقات) من قبل

التعرض لمخاطر رقمية	الإجمالي	
	ك	%
نعم	30	21.9%
لا	107	78.1%
الإجمالي	137	100%

تشير نتائج الجدول رقم (13) إلى الصحفيين الذي تعرضوا لمخاطر رقمية سابقة، حيث أفاد (21.9 %) منهم إلى تعرضهم لمخاطر رقمية، بينما أشار (78.1%) منهم إلى عدم تعرضهم لمخاطر رقمية سابقة.

ومن خلال إتاحة تساؤل مفتوح للصحفيين حول طبيعة هذه المخاطر، كان الإجماع على أن المخاطر الرقمية تتمثل في الاختراق المتكرر لحسابات مواقع التواصل الاجتماعي (فيسبوك تحديدا)، ومحاولة اختراق البريد الإلكتروني، وأفاد البعض أن اختراق حساب فيسبوك، والسطو على الهوية، كان بهدف خداع الأصدقاء وطلب مبالغ مالية منهم.

أما **الإجراءات التي تم اعتمادها عند تعرضهم للاختراق** فتنوعت بين الاستعانة بشخص متخصص لمحاولة إرجاع الحساب، أو اتباع الخطوات الرسمية لاسترجاع الحساب، وتأمين الحساب من خلال تغيير كلمة المرور، ولجوء البعض لإجراءات أكثر أمنًا لتسجيل الدخول، مثل ربط البريد والحساب برقم الهاتف، والحذر من البرامج التي يتم تثبيتها، والحرص على إعلام الزملاء بتعرض الحساب للاختراق، في حين قام أحد الصحفيين بتقديم بلاغ رسمي لمباحث الإنترنت.

جدول رقم (14) يوضح ما إذا كانت المخاطر الرقمية تقف عقبة أمام استخدام الصحفيين للوسائل الرقمية

هل تقف المخاطر عقبة أمام استخدامك للوسائل الرقمية	الإجمالي	
	ك	%
نعم	39	28.5%
لا	98	71.3%
الإجمالي	137	100%

تشير نتائج الجدول رقم (14) إلى أن هذه المخاطر الرقمية لم تقف في الأغلب كعقبة أمام استخدام الصحفي للوسائل الرقمية، حيث أفاد بذلك (71.3 %) منهم، بينما يرى (28.5 %) من الصحفيين أنها قد تقف عقبة أمام استخدامهم للوسائل الرقمية.

مما يعني أن تقييم مخاطر التكنولوجيا الرقمية مسألة هامة، إلا أنها لا تقف عقبة أمام النظر إلى المنافع العديدة والفوائد العظيمة لها، لذلك يتطلب الأمر رفع درجة الوعي بها، وتحديد الإستراتيجيات التي تجعل الحياة الرقمية للأشخاص أكثر أمنًا.

وتتفق هذه النتائج، جزئيًا، مع نتائج دراسة (Mitchell A., et al., 2015)، حيث تؤكد الغالبية العظمى على أن فوائد الاتصالات الرقمية تفوق المخاطر، ورغم ذلك كان الخوف من التتبع سببًا في توقفهم عن إجراء بعض التحقيقات، أو الوصول إلى مصادر محددة.

ثالثا: دور المؤسسات الصحفية في دعم مفهوم الأمن الرقمي:

جدول رقم (15) يوضح مشاركة المبحوثين في دورات تدريبية في مجال الأمن الرقمي

المشاركة في دورات تدريبية	الإجمالي	
	ك	%
نعم	37	27%
لا	100	73%
الإجمالي	137	100%

تشير نتائج الجدول رقم (15) إلى أن أغلب الصحفيين، عينة الدراسة، لم يحصلوا مسبقًا على دورات تدريبية خاصة بالأمن الرقمي، حيث أفاد بذلك (73 %) من العينة، بينما حصل (27 %) منهم على دورات تدريبية.

وتتفق هذه النتيجة مع نتائج دراسة (Internews Center, 2012)، حيث لم يحظ معظم الصحفيين بفرصة تدريب على كيفية ضمان أمنهم الرقمي، كما تتفق مع نتائج دراسة (Çalışkan B., 2019)، ودراسة (Olunifesi S. and Olawale O., 2017)، حيث يتطلع الصحفيون للحصول على دورات تدريبية.

جدول رقم (16) يوضح طبيعة التدريب الذي تلقاه المبحوثون

طبيعة التدريب	الإجمالي	
	ك	%
تعلم ذاتي	22	16.1%
دورات تدريبية بواسطة مؤسسات	14	10.2%
حملات المعلومات على الإنترنت	1	0.7%
الإجمالي	ن = 37	

تشير نتائج الجدول رقم (16) إلى أن التعلم الذاتي لبعض الصحفيين في الترتيب الأول بنسبة (16.1 %)، ثم تلقي تدريب بواسطة مؤسسات مختلفة حول الأمن الرقمي، حيث أفاد بذلك نسبة (10.2 %)، بينما اهتمت نسبة (0.7 %) بمتابعة حملات المعلومات التي تتوافر على الإنترنت.

ويمكن أن تعكس نتيجة هذا الجدول أن بعض الصحفيين لديهم عقلية أمنية متقدمة، دفعتهم إلى أن يكونوا أكثر وعيًا بكيفية حماية أنفسهم عبر محاولات التعلم الذاتي للأمن الرقمي.

تتفق هذه النتيجة، بصورة كبيرة، مع دراسة (Tsui L., and Francis L., 2019)، حيث لم يحصل الصحفيون على دورات تدريبية حول الأمن الرقمي من قبل المؤسسات الصحفية على الإطلاق، حيث تم تعلم مهارات ومعارف مجال الأمن الرقمي من خلال التفاعل مع الأقران والتعلم الذاتي، كما تتفق مع نتائج دراسة (Shere A., et. al. 2020)، حيث ذهبت إلى الحاجة إلى إعطاء التدريب أولوية لدى المؤسسات الصحفية.

جدول رقم (17) يوضح ما إذا كانت الصحيفة توفر دعمًا فنيًا لمساعدة الصحفيين

الدعم الفني داخل المؤسسة	الإجمالي	
	ك	%
نعم	107	78.1%
لا	30	21.9%
الإجمالي	137	100%

تشير نتائج الجدول رقم (17) إلى رؤية الصحفيين حول ما إذا كانت الصحيفة تخصص شخصًا مسئولا عن المسائل الفنية، يمكن اللجوء إليه في حال الحاجة لمساعدة رقمية ما، وقادر على إدارة حالات الطوارئ على الفور، حيث يرى (78.1 %) أن أغلب المؤسسات الصحفية توفر دعمًا فنيًا لصحفييها يمكنهم الاستعانة به، بينما أفاد (21.9 %) من الصحفيين

بعدم توفير المؤسسات الصحفية لدعم فني.

ومن خلال إتاحة سؤال مفتوح للمبحوثين، لشرح المزيد حول أشكال الدعم الذي توفره المؤسسات الصحفية لهم من دعم، كانت استجاباتهم على النحو التالي:

- توفر المؤسسات الصحفية جدار الحماية الناري Fire Wall للحماية من المواقع غير الآمنة.
- أفاد البعض أن المؤسسة لا تقدم دعمًا كافيًا، وقد وصفه البعض بعبارات (دعم مقبول، دعم بسيط، لا تقدم شيئًا، تقدم دعم بنسبة 50 %، تقدم دعم 2 على 10، دعم ضعيف، دعم ليس كبيرًا، يطلب مني مهندس الدعم الفني عمل إعادة تشغيل للجهاز restart كلما تعرض الجهاز لأي مشكلة، هم أنفسهم يخترقون خصوصية الصحفيين).
- توفر المؤسسة الدعم الأمني تجاه عدم اختراق المؤسسة من الخارج فقط.
- تأمين أجهزة العمل يكون عن طريق وضع كلمة مرور شخصية لكل جهاز.

الاحتياجات التدريبية للمبحوثين:

تنوعت استجابات الصحفيين عينة الدراسة تجاه الاحتياجات التي يرغبون في تعزيزها على النحو التالي:

- تقييم للمخاطر الرقمية المحتملة.
- إدارة كلمات المرور.
- مهارات الحفاظ على خصوصية الاتصالات.
- تأمين الحسابات الشخصية.
- الحفاظ على خصوصية الهاتف.

تتفق هذه النتيجة مع نتائج دراسة (Olunifesi S. & Olawale O., 2017)، حيث الحاجة للتدريب على الأمن الرقمي؛ لمعالجة الفجوة المعرفية الملحوظة، وإعطاء الأولوية لإعدادات الأمان لحساباتهم على وسائل التواصل الاجتماعي والأجهزة الرقمية، وتتفق أيضا مع نتائج دراسة (Shere A., et. al. 2020) ، ونتائج دراسة (Internews Center, 2012) حيث أظهر

الصحفيون الحاجة إلى التدريب على أدوات الأمن الرقمي.

رابعا: إستراتيجيات الأمن الرقمي:

هناك مجموعة من الأدوات الخاصة بالأمن الرقمي، التي يمكن للأفراد الذين يستخدمون المنصات والأدوات الرقمية استخدامها لرفع درجة الأمان في الاستخدام، وتقليل المخاطر قدر المستطاع، ويوضح الجدول التالي رقم (18) مدى معرفة الصحفيين عينة الدراسة ببعض هذه الأدوات، وتعني المعرفة هنا العلم بالأداة وليس الاستخدام الفعلي لها، فمن الممكن أن يكون لدى الفرد معرفة بوجود طرق لإخفاء عنوان IP أثناء التصفح، إلا أنه لا يقوم بذلك، بينما يقيس الجدول رقم (21) استخدامهم الفعلي لهذه الأدوات.

جدول رقم (18) معرفة المبحوثين لأدوات تعزيز الأمن الرقمي

العبارات	درجة المعرفة						الإجمالي		المتوسط الحسابي	الانحراف المعياري
	لا		أحيانا		نعم					
	ك	%	ك	%	ك	%	ك	%		
إدارة كلمات مرور قوية	5	3.6	17	12.4	115	83.9	137	100%	2.8029	0.48263
المصادقة الثنائية	5	3.6	31	22.6	101	73.7	137	100%	2.7007	0.53365
التغيير الدائم لكلمات المرور	7	5.1	52	38	78	56.9	137	100%	2.5182	0.59535
برامج مكافحة الفيروسات	14	10.2	47	34.3	76	55.5	137	100%	2.4526	0.67487
عدم استخدام كلمة مرور واحدة	21	15.3	39	28.5	77	56.2	137	100%	2.4088	0.74315
استخدام البرامج الأصلية	35	25.5	56	40.9	46	33.6	137	100%	2.0803	0.76752
فحص مرفقات البريد	41	29.9	53	38.7	43	31.4	137	100%	2.0146	0.78577
التصفح المخفي	47	34.3	52	38	38	27.7	137	100%	1.9343	0.78782
تطبيقات المحادثة المشفرة	59	43.1	39	28.5	39	28.5	137	100%	1.854	0.83613
جدار الحماية الناري	57	41.6	44	32.1	36	26.3	137	100%	1.8467	0.8125
معيار وجود علامة القفل	61	44.5	36	26.3	40	29.2	137	100%	1.8467	0.84793
الحذف الآمن	57	41.6	45	32.8	35	25.5	137	100%	1.8394	0.80653
تشفير البيانات	61	44.5	46	33.6	30	21.9	137	100%	1.7737	0.78584
إخفاء عنوان IP	72	52.6	32	23.4	33	24.1	137	100%	1.7153	0.83092

متصفح تور	67	48.9	48	35	22	16.1	137	100%	1.6715	0.73873
تشفير البريد الإلكتروني	73	53.3	38	27.7	26	19	137	100%	1.6569	0.78063
هاتف مشفر	78	56.9	29	21.2	30	21.9	137	100%	1.6496	0.81882
الشبكات الافتراضية	76	55.5	41	29.9	20	14.6	137	100%	1.5912	0.73319

جاء في الترتيب الأول لدرجة معرفة المبحوثين لأدوات الأمن الرقمي **استخدامهم لكلمات مرور قوية**، بمتوسط حسابي قدره 2.8029، يليه **استخدام المصادقة الثنائية (التحقق عبر خطوتين)** من خلال طلب إرسال كود عبر SMS على الهاتف المحمول، كخطوة إضافية للدخول إلى الحساب مع كلمة المرور، وذلك بمتوسط حسابي 2.7007، وفي الترتيب الثالث كان متغير **التغيير الدائم لكلمات المرور** بمتوسط 2.5182، ثم **استخدام برامج مكافحة الفيروسات** بمتوسط قدره 2.4526، ثم عدم **استخدام كلمة مرور واحدة لجميع الحسابات** بمتوسط 2.4088، ثم **استخدام البرامج الأصلية عوضًا عن البرامج المجانية المتوافرة على مواقع الإنترنت** بمتوسط 2.0803، ثم فحص مرفقات البريد الإلكتروني بمتوسط 2.0146، ثم التصفح المخفي عبر Private browsing بمتوسط 1.9343، ثم استخدام التطبيقات التي تمنح محادثة مشفرة ودردشة سرية وميزة التدمير الذاتي للرسائل مثل Telegram بمتوسط 1.854، ثم استخدام جدار الحماية الناري (الشهير باسم Firewall) بمتوسط 1.8467، ثم التأكد من معيار وجود علامة القفل والأحرف https في عنوان الموقع URL بمتوسط 1.8467، ثم الحذف الآمن والنهائي للملفات عبر البرامج الخاصة بحيث لا يمكن استرجاعها مرة أخرى بمتوسط 1.8394، ويستمر الانخفاض الملحوظ في معرفة الصحفيين ببعض الأدوات الخاصة بالأمن الرقمي مثل تشفير البيانات على التخزين السحابي أو القرص الصلب بمتوسط 1.7737، واستخدام أدوات لإخفاء عنوان IP بمتوسط 1.7153، واستخدام متصفح تور للمجهولية Tor بمتوسط 1.6715،

وتشفير البريد الإلكتروني عبر استخدام أدوات مثل: GPG, Mailvelope بمتوسط 1.6569، واستخدام هاتف مشفر 1.6496، والاعتماد على الشبكات الافتراضية (المعروفة باسم Virtual Private Network – VPN والتي من أشهر أسباب استخدامها الدخول إلى مواقع محجوبة أو للتواصل بشكل آمن) بمتوسط 1.5912.

ويوضح الجدول التالي رقم (19) مقياس معرفة المبحوثين بأدوات الأمن الرقمي

مقياس المعرفة بأدوات الأمن الرقمي	الإجمالي		المتوسط الحسابي	الانحراف المعياري
	ك	%		
منخفض	28	20.4%	1.9489	0.59805
متوسط	88	64.2%		
مرتفع	21	15.3%		
الإجمالي	137	100%		

تدل نتائج هذا الجدول على أن المقياس العام لمعرفة الصحفيين بالأدوات الرقمية هو **المعرفة المتوسطة**، حيث تم بناء هذا المقياس من 18 عبارة، حيث قدرت الإجابات: نعم=3، محايد=2، معارض=1، وبالتالي فإن محصلة هذا المقياس تتكون من (37) درجة من 17 : 54، تم تقسيمها إلى ثلاثة مستويات، مستوى منخفض (18 : 30)، مستوى متوسط (31 : 42)، ومستوى مرتفع (43 : 54).

ومن خلال نتائج الجدولين السابقين (18) و(19) يمكن القول باعتبار أن معرفة الصحفيين للإجراءات البسيطة المتاحة لجميع مستخدمي الأدوات والمنصات الرقمية مثل (الاهتمام بكلمات المرور سواء عبر اختيار كلمات مرور قوية، أو تغيير الدائم لها، أو عدم استخدام كلمة مرور واحدة لجميع الحسابات، المصادقة الثنائية، وفحص مرفقات البريد) أعلى من معرفتهم

للإجراءات الأكثر تخصصًا وصعوبة وربما تعقيدا، مثل (استخدام الشبكات الافتراضية، أو التشفير سواء استخدام هاتف مشفر أو تشفير البريد الإلكتروني أو تشفير البيانات الرقمية)، والتي تحتاج إلى مزيد من البحث المتخصص عن أدوات الحماية، مما يدلل على أن الصحفيين بحاجة إلى مزيد من المعرفة للأدوات التي يمكن أن تمنحهم حماية أكبر.

تتفق هذه النتائج مع نتائج دراسة (Internews Center, 2012)، حيث يرى المبحوثون أن كلمات المرور القوية ومضاد الفيروسات من أعلى الأدوات التي قد تمثل فائدة في الأمن الرقمي، بينما لا يرون أهمية كبيرة للتشفير أو استخدام حظر IP أو لاستخدام VPN.

جدول رقم (20) يوضح العلاقة بين معرفة المبحوثين بأدوات الأمن الرقمي وبين الصحف التي ينتمون إليها

المعرفة	أخبار اليوم		اليوم السابع		الوطن		الشروق		الوفد		الإجمالي	
	ك	%	ك	%	ك	%	ك	%	ك	%	ك	%
منخفض	3	9.1%	11	29.7%	11	33.3%	2	12.5%	1	5.6%	28	20.4%
متوسط	27	81.8%	21	56.8%	19	57.6%	9	56.3%	12	66.7%	88	64.2%
مرتفع	3	9.1%	5	13.5%	3	9.1%	5	31.3%	5	27.8%	21	15.3%
الإجمالي	33	100%	37	100%	33	100%	16	100%	18	100%	137	100%

كا2=17.305 درجات الحرية=8 مستوى الدلالة=0.027 معامل التوافق=0.335

تشير النتائج إلى وجود فروق ذات دلالة إحصائية بين مستوى المعرفة بين الصحفيين في الصحف محل عينة الدراسة، حيث بإجراء اختبار قيمة كا2=17.305، تبين وجود فروق ذات دلالة إحصائية بين الصحف عينة الدراسة والمعرفة، وهي دالة عند مستوى معنوية 0.027، وقد بلغ معامل التوافق 0.335، أي أن هناك اختلافات بين الصحف عينة الدراسة فيما يتعلق بدرجة معرفتهم للأدوات الخاصة بالأمن الرقمي، إلا أن هذه العلاقة

تعد متوسطة، حيث يتم تفسير معامل التوافق (أقل من 0.333 علاقة ضعيفة، من 0.333 : 0.666 علاقة متوسطة، أكبر من 0.666 علاقة قوية).

جدول رقم (21) يوضح استخدامات المبحوثين لأدوات الأمن الرقمي

العبارات	درجة الاستخدام						الإجمالي		المتوسط الحسابي	الانحراف المعياري
	لا استخدمها		أحيانا		دائما					
	ك	%	ك	%	ك	%	ك	%		
أفضل المقابلة وجهًا لوجه لتخفيف المخاطر	9	6.6	39	28.5	89	65	137	100	2.5839	0.61408
إدارة كلمات مرور قوية	14	10.2	37	27	86	62.8	137	100	2.5255	0.67606
عدم استخدام كلمة مرور واحدة لجميع الحسابات	29	21.2	38	27.7	70	51.1	137	100	2.2993	0.79857
لا حاجة للخوف من المخاطر الرقمية	18	13.1	69	50.4	50	36.5	137	100	2.2336	0.66711
برامج مكافحة الفيروسات	36	26.3	37	27	64	46.7	137	100	2.2044	0.8326
نسخة احتياطية	35	25.5	50	36.5	52	38	137	100	2.1241	0.79006
التغيير الدائم لكلمات المرور	31	22.6	60	43.8	46	33.6	137	100	2.1095	0.74438
المصادقة الثنائية	38	27.7	47	34.3	52	38	137	100	2.1022	0.807
استخدام البرامج الأصلية	35	25.5	60	43.8	42	30.7	137	100	2.0511	0.7507
أقرأ سياسة الخصوصية	37	27	56	40.9	44	32.1	137	100	2.0511	0.77004
أفضل عدم العمل على موضوعات حساسة	41	29.9	51	37.2	45	32.8	137	100	2.0292	0.79467
فحص مرفقات البريد	37	27	59	43.1	41	29.9	137	100	2.0292	0.75675

الحذف الآمن	47	34.3	53	38.7	37	27	137	100	1.927	0.78248
معيار وجود علامة القفل	60	43.8	38	27.7	39	28.5	137	100	1.8467	0.83921
التصفح المخفي	65	47.4	28	20.4	44	32.1	137	100	1.8467	0.88193
جدار الحماية الناري	65	47.4	39	28.5	33	24.1	137	100	1.7664	0.81586
تطبيقات محادثة مشفر	69	50.4	39	28.5	29	21.2	137	100	1.708	0.79669
تشفير البيانات	75	54.7	47	34.3	15	10.9	137	100	1.562	0.68451
إخفاء عنوان IP	90	65.7	18	13.1	29	21.2	137	100	1.5547	0.82176
متصفح تور	98	71.5	21	15.3	18	13.1	137	100	1.4161	0.71375
هاتف مشفر	93	67.9	32	23.4	12	8.8	137	100	1.4088	0.64801
تشفير البريد الإلكتروني	108	78.8	14	10.2	15	10.9	137	100	1.3212	0.66348
الشبكات الافتراضية VPN	105	76.6	22	16.1	10	7.3	137	100	1.3066	0.601

جاءت استجابات المبحوثين للإجراءات أو الأدوات الفعلية التي يستخدمونها من أجل تعزيز أمنهم الرقمي على النحو التالي: **أفضل المقابلة وجهًا لوجه لتخفيف المخاطر** في الترتيب الأول بمتوسط (2.5839)، ثم **إدارة كلمات مرور قوية** بمتوسط (2.5255)، ثم **عدم استخدام كلمة مرور واحدة لجميع الحسابات** بمتوسط (2.2993)، ثم **لا حاجة للخوف من المخاطر الرقمية** بمتوسط (2.2336)، ثم **برامج مكافحة الفيروسات** بمتوسط (2.2044)، ثم **الاحتفاظ بنسخة احتياطية** بمتوسط (2.1241)، ثم **التغيير الدائم لكلمات المرور** بمتوسط (2.1095)، ثم **المصادقة الثنائية (التحقق عبر خطوتين) من خلال طلب إرسال كود عبر SMS على الهاتف المحمول كخطوة إضافية للدخول إلى الحساب مع كلمة المرور** بمتوسط (2.1022)، ثم **استخدام البرامج الأصلية** بمتوسط (2.0511)، ثم أقرأ سياسة الخصوصية بمتوسط (2.0511)، ثم أفضل عدم العمل على موضوعات حساسة بمتوسط (2.0292)، ثم فحص مرفقات البريد بمتوسط

(2.0292)، ثم الحذف الآمن بمتوسط (1.927)، ثم معيار وجود علامة القفل بمتوسط (1.8467)، ثم التصفح المخفي بمتوسط (1.8467)، ثم جدار الحماية الناري بمتوسط (1.7664)، ثم تطبيقات المحادثة المشفرة بمتوسط (1.708)، ثم تشفير البيانات بمتوسط (1.562)، ثم إخفاء عنوان IP بمتوسط (1.5547)، ثم متصفح تور بمتوسط (1.4161)، ثم هاتف مشفر بمتوسط (1.4088)، ثم تشفير البريد الإلكتروني بمتوسط (1.3212)، ثم الشبكات الافتراضية بمتوسط (1.3066).

تدلل هذه النتيجة على أن كثيرًا من الصحفيين ينتهجون إستراتيجية الدفاع غير الرقمي، من خلال المقابلة وجهًا لوجه لتخفيف مخاطر تداول البيانات أو الاتصالات، أما الإستراتيجيات الرقمية فيمكن تقسيمها من خلال هذه النتائج إلى إستراتيجيات بسيطة، متمثلة في استخدام الأدوات التقليدية للحفاظ على الأمن الرقمي، مثل العناية باختيار كلمات المرور، واختيار طرق المصادقة الثنائية، واستخدام برامج مكافحة الفيروسات، والاحتفاظ بنسخ احتياطية من الملفات، بينما تمنح بعض الأدوات المتقدمة مزيدًا من الأمن الرقمي إلا أن استخدام الصحفيين لها أقل من اعتمادهم على الطرق البسيطة، مثل استخدام شبكات تور (تعتبر Tor شبكة لحماية الخصوصية الشخصية وأنشطة الأعمال الخاصة والعلاقات الفردية وإخفاء الهوية، كما يوفر الحماية أيضا من الممارسات المعروفة بتحليل حركة المرور، حيث تمكن هذه الشبكة المستخدمين من الاتصال بالإنترنت عبر سلسلة من الأنفاق الافتراضية بدلا من الاتصالات المباشرة، مما يتيح للمستخدمين مشاركة المعلومات عبر الشبكات العامة، أو القيام بالمراسلات الفورية دون التضحية بالخصوصية)، ومن الأدوات الهامة أيضا تشفير البيانات بشكل آمن، لضمان خصوصية وأصالة رسائل البريد الإلكتروني المرسلة أو المستقبلة، إلا أن اعتماد الصحفيين عليها أيضا منخفض، مما قد يدلل على ضعف القدرة على اتخاذ الإجراءات الأكثر أمنا وفعالية، نظرا لضعف الإمكانات التقنية لديهم.

تتفق هذه النتيجة مع دراسة (Internews Center, 2012)، حيث كانت أعلى الإستراتيجيات المستخدمة هي استخدام كلمات مرور قوية ومضادات الفيروسات، وتحديث أنظمة التشغيل بصورة دائمة، بينما يقل الاعتماد على التشفير وشبكات VPN، كما تتفق مع نتائج دراسة (Sierra J., 2013)، حيث يضعف الاعتماد على استخدام أدوات الحماية الرقمية المتقدمة، مثل التشفير، واستخدام الشبكات الافتراضية الخاصة VPNs، وحذف الملفات بشكل آمن، وتتفق جزئيا مع نتائج دراسة (McGregor and Watkins, 2016)، حيث يرى بعض الصحفيين أن سبيل الحماية يكون من خلال العمل على الأخبار غير الحساسة، وتتفق أيضا مع نتائج دراسة (Shere A., et. al. 2020)، حيث كان النهج الأساسي الذي يميل إليه بعض الصحفيين تجاه حماية أنفسهم هو النهج التقليدي.

ويوضح الجدول التالي رقم (22) مقياس استخدام الصحفيين لأدوات الأمن الرقمي

مقياس استخدام أدوات الأمن الرقمي	الإجمالي		المتوسط الحسابي	الانحراف المعياري
	ك	%		
منخفض	37	27.0%	1.8248	0.58029
متوسط	87	63.5%		
مرتفع	13	9.5%		
الإجمالي	137	100%		

يدل المقياس العام لاستخدامات الصحفيين لأدوات الأمن الرقمي على الاستخدام **المتوسط**، حيث تم بناء هذا المقياس من 23 عبارة حيث قدرت الإجابات: نعم= 3، محايد=2، معارض=1، وبالتالي فإن محصلة هذا المقياس تتكون من (47) درجة؛ 23 : 69، تم تقسيمها إلى ثلاثة مستويات، مستوى منخفض (23 : 38)، مستوى متوسط (39 : 54)، ومستوى مرتفع (55 : 69).

جدول رقم (23) يوضح العلاقة بين استخدام الصحفيين لأدوات الأمن الرقمي وبين الصحف التي ينتمون إليها

درجة المعرفة الرقمية	أخبار اليوم		اليوم السابع		الوطن		الشروق		الوفد		الإجمالي	
	ك	%	ك	%	ك	%	ك	%	ك	%	ك	%
منخفض	7	21.2%	14	37.8%	5	15.2%	4	25.0%	7	38.9%	37	27.0%
متوسط	25	75.8%	22	59.5%	26	78.8%	6	37.5%	8	44.4%	87	63.5%
مرتفع	1	3.0%	1	2.7%	2	6.1%	6	37.5%	3	16.7%	13	9.5%
الإجمالي	33	100%	37	100%	33	100%	16	100%	18	100%	137	100%

كا2=27.385 درجات الحرية=8 مستوى الدلالة=0.001 معامل التوافق=0.408

تشير النتائج إلى وجود فروق ذات دلالة إحصائية بين مستوى المعرفة بين الصحفيين في الصحف محل عينة الدراسة، بإجراء اختبار قيمة كا2=27.385 تبين وجود فروق ذات دلالة إحصائية بين الصحف عينة الدراسة والمعرفة، وهي دالة عند مستوى معنوية 0.001، وقد بلغ معامل التوافق 0.408، أي أن هناك اختلافات واضحة بين الصحف عينة الدراسة فيما يتعلق بدرجة معرفتهم للأدوات الخاصة بالأمن الرقمي، وتعتبر شدة هذه العلاقة متوسطة.

جدول رقم (24) يوضح التحديات التي يواجهها المبحوثون وقد تقف عقبة أمام تحقيق أمنهم الرقمي

العبارات	درجة الموافقة						الإجمالي		المتوسط الحسابي	الانحراف المعياري
	معارض		محايد		موافق			
	ك	%	ك	%	ك	%	ك	%		
كثير من أدوات الأمن الرقمي ليست سهلة الاستخدام	6	4.4	37	27	94	68.6	137	100	0.6423	0.56539

لا يستخدم هذه الأدوات عدد كاف من الأفراد الذين أعرفهم	12	8.8	35	25.5	90	65.7	137	100	0.5693	0.65074
ارتفاع تكلفة شراء البرامج التجارية التي ترفع مستوى الأمن الرقمي	8	5.8	43	31.4	86	62.8	137	100	0.5693	0.60386
لا تستخدم المصادر التي أتعامل معها هذه التقنيات	8	5.8	51	37.2	78	56.9	137	100	0.5109	0.60775
نقص البيانات التي توثق أنواع الهجمات الرقمية والتهديدات التي تواجه الصحفيين	10	7.3	59	43.1	68	49.6	137	100	0.4234	0.62688
تخلق حاجزا للتواصل مع المصادر	15	10.9	51	37.2	71	51.8	137	100	0.4088	0.68121
لا توفر أدوات الأمن الرقمي الدفاع اللازم	7	5.1	73	53.3	57	41.6	137	100	0.365	0.58001
من الصعب تقييم مصداقية –أمن– الأداة	13	9.5	66	48.2	58	42.3	137	100	0.3285	0.64294
التقنيات الخاصة بالأمن معقدة جدا	12	8.8	72	52.6	53	38.7	137	100	0.2993	0.62267
الدعم التقني غير كاف من المؤسسة التي أعمل بها	33	24.1	37	27	67	48.9	137	100	0.2482	0.82052
لست على علم تمامًا بالمهام الأمنية التي أحتاج إليها	25	18.2	58	42.3	54	39.4	137	100	0.2117	0.73195
العمل الصحفي ليس حساسًا لهذه الدرجة	53	38.7	61	44.5	23	16.8	137	100	0.219-	0.71451

تشير بيانات الجدول السابق (24) إلى أن أهم التحديات التي قد تقف عقبة أمام الصحفيين أن كثيرًا من **أدوات الأمن الرقمي ليست سهلة الاستخدام** في الترتيب الأول بمتوسط (0.6423)، ثم **لا يستخدم هذه الأدوات عدد كاف من الأفراد الذين أعرفهم** في الترتيب الثاني بمتوسط (0.5693)، ثم **ارتفاع تكلفة شراء البرامج التجارية التي ترفع مستوى الأمن الرقمي** بمتوسط (0.5693)، ثم **لا تستخدم المصادر التي أتعامل معها هذه التقنيات** بمتوسط (0.5109)، ثم **نقص البيانات التي توثق أنواع الهجمات الرقمية والتهديدات التي تواجه الصحفيين** بمتوسط (0.4234)، يليها عبارات: تخلق حاجزا للتواصل مع المصادر التي لا تعتمد على التقنيات المشابهة، بمتوسط (0.4088)، لا توفر أدوات الأمن الرقمي الدفاع اللازم، بمتوسط (0.365)، من الصعب تقييم مصداقية –أمن- الأداة، بمتوسط (0.3285)، التقنيات الخاصة بالأمن معقدة جدًا، بمتوسط (0.2993)، الدعم التقني غير كاف من المؤسسة التي أعمل بها، بمتوسط (0.2482)، لست على علم تمامًا بالمهام الأمنية التي أحتاج إليها بمتوسط (0.2117)، العمل الصحفي ليس حساسًا لهذه الدرجة (لا أحد يبحث عني)، بمتوسط (-0.219).

ويمكن تفسير هذه النتائج بأن معيار سهولة الاستخدام تمثل عاملا رئيسيًا في تبني الصحفيين لأدوات الأمن الرقمي، حيث يعتقد الصحفيون أن أدوات الأمان، المتقدمة تحديدا كما ورد بالجدولين 19، 21، معقدة وصعبة الاستخدام، مما يقلل الاعتماد عليها، كما يعد عائق عدم شيوع الاستخدام أيضا بالنسبة للأفراد الذين يتعامل معهم الصحفي تحديًا هامًّا أمام تبنيه لهذه الوسائل، ويمكن ربط هذه النتيجة مع ضعف اهتمام المؤسسات الصحفية نحو تثقيف صحفييها حول الأمن الرقمي، وتدريبهم على المخاطر المحتملة، وتحديد الآليات التي ينبغي العناية بها، والتدابير الأمنية التي ينبغي أن يختاروها، مما جعلها مبهمة وصعبة بالنسبة إليهم.

وتتفق النتائج الخاصة بشعور الصحفيين أن عملهم ليس حساسًا للدراسة التي تجعلهم يواجهون تهديدات رقمية، مع نتائج دراسة (McGregor and Watkins, 2016) حيث لدى الصحفيين الوعي بوجود تهديدات ومخاطر

رقمية، إلا أن بعضهم يعتقد بعدم احتياجهم اتخاذ احتياطات أمنية، ما لم يشاركوا في عمل حساس بدرجة كافية لجذب انتباه الجهات الفاعلة نحوهم، كما تتفق مع نتائج دراسة (Franziska Roesner, et al. 2015)، حيث كان الاعتماد المحدود على أدوات الأمان بسبب تحديات قابلية هذه الأدوات الاستخدام.

جدول رقم (25) يوضح مقياس تحديات استخدام الصحفيين لأدوات الأمن الرقمي:

تحديات استخدام أدوات الأمن الرقمي	الإجمالي		المتوسط الحسابي	الانحراف المعياري
	ك	%		
منخفض	3	2.2%	2.6277	0.52870
متوسط	45	32.8%		
مرتفع	89	65%		
الإجمالي	137	100%		

تعد اتجاهات الصحفيين نحو التحديات التي تمثل عائقًا أمام تبنيهم لمزيد من الإجراءات التي تعزز من أمنهم الرقمي اتجاهًا **مرتفعًا**؛ حيث تم بناء هذا المقياس من 12 عبارة، حيث قدرت الإجابات: نعم=1، محايد=0، معارض=(-1)، وبالتالي فإن محصلة هذا المقياس تتكون من (25) درجة؛ (-12) : 12، تم تقسيمها إلى ثلاثة مستويات، مستوى منخفض (-12 : -4)، مستوى متوسط (-3 : 3)، ومستوى مرتفع (4 : 12).

جدول رقم (26) يوضح العلاقة بين رؤية الصحفيين للتحديات وبين الصحف التي ينتمون إليها

درجة المعرفة الرقمية	أخبار اليوم		اليوم السابع		الوطن		الشروق		الوفد		الإجمالي	
	ك	%	ك	%	ك	%	ك	%	ك	%	ك	%
منخفض	0	0%.	1	2.7%	0	0%.	0	0%.	2	11.1%	3	2.2%
متوسط	11	33.3%	18	48.6%	4	12.1%	5	31.3%	7	38.9%	45	32.8%
مرتفع	22	66.7%	18	48.6%	29	87.9%	11	68.8%	9	50.0%	89	65.0%
الإجمالي	33	100%	37	100%	33	100%	16	100%	18	100%	137	100%

كا2=20.579 درجات الحرية=8 مستوى الدلالة=0.008 معامل التوافق=0.361

تشير النتائج إلى وجود فروق ذات دلالة إحصائية، بين مستوى المعرفة بين الصحفيين في الصحف محل عينة الدراسة، بإجراء اختبار قيمة كا2=20.579 تبين وجود فروق ذات دلالة إحصائية بين الصحف عينة الدراسة والمعرفة، وهي دالة عند مستوى معنوية 0.008، وقد بلغ معامل التوافق 0.361، أي أن هناك اختلافات واضحة بين الصحف عينة الدراسة فيما يتعلق بدرجة معرفتهم للأدوات الخاصة بالأمن الرقمي، وتعتبر شدة هذه العلاقة متوسطة.

اختبار الفروض:

الفرض الأول: توجد علاقة بين معرفة الصحفيين بالأساليب والأدوات الخاصة بالأمن الرقمي وبين استخدامهم الفعلي لها.

		مقياس درجة المعرفة
مقياس درجة الاستخدام	معامل الارتباط	0.631
	مستوى الدلالة	0.000
	ن	137

تشير هذه البيانات إلى وجود علاقة ارتباط طردية متوسطة، بين معرفة الصحفيين بأدوات الأمن الرقمي، وبين استخدامهم لها، حيث بلغت

قيمة معامل ارتباط بيرسون= 0.631، وهي دالة عند مستوى معنوية= 0.000، أي أنه كلما زادت درجة المعرفة بأدوات الأمن الرقمي ازدادت درجة الاستخدام لها.

مما قد يدلل على أن ضعف ممارسات الأمن الرقمي لدى الصحفيين ينبع من نقص المعرفة لديهم بالإجراءات الأخرى الأكثر فعالية، وهو ما يمكن تحسينه بالتدريب المناسب، حيث إنه نظرًا لأن الصحفيين في العينة يستخدمون في الواقع أدوات الأمن الرقمي التي يعرفونها بالفعل، مثل برامج مكافحة الفيروسات واستخدام كلمات مرور قوية، فإن ذلك يمكن أن يعكس استعدادهم لوضع المعرفة الأمنية موضع التنفيذ إذا كانت لديهم المعلومات التي يحتاجونها، والقدرة على الاستعانة بمثل هذه التكنولوجيا المتقدمة.

لذلك يمكن التأكيد على أن مجرد المعرفة لا يكفي للحصول على الأمن الرقمي، حيث لا بد أن يتبعها القيام بإجراءات فعلية، وأن معظم الصحفيين في جميع أنحاء العالم لا يستخدمون أدوات الأمن الرقمي، رغم أنهم على وعي بالتهديدات والمخاطر الرقمية المحتملة، حيث لم يحظوا بفرص تدريبية أو بمناهج دراسية تعليمية تمكنهم من تشبيك التعلم بالتطبيق.

وتتفق هذه النتيجة مع نتائج دراسة (Olunifesi S. & Olawale O., 2017)، ونتائج دراسة (Internews Center, 2012)، حيث يكتفي الصحفيون بالاعتماد على إستراتيجيات الأمن البسيطة، مثل تغيير واستخدام كلمات مرور قوية، والحفاظ على أجهزة الكمبيوتر الخاصة بهم آمنة من فيروسات الإنترنت؛ عن إستراتيجيات الأمان المتقدمة، مثل حجب عناوين IP، وهو ما يُعزى أيضا إلى مهاراتهم التقنية المحدودة. كما تتفق نتائج هذه الدراسة جزئيًا مع نتائج دراسة (Çalışkan B., 2019)، حيث لم تنعكس معرفة الصحفيين بأدوات الأمن الرقمي على استخداماتهم الفعلية لها، حيث لم يتجاوز مدى معرفتهم بالأدوات سوى الأدوات التقليدية أيضا، مثل استخدام كلمات مرور قوية، ويفتقر معظم المستجيبين إلى فهم مستوى الأمان الذي توفره الأدوات والتقنيات الأكثر تعقيدا، وتتفق جزئيًا أيضا مع نتائج دراسة

(SecondMuse, 2014)، حيث إدراك الصحفيين لإستراتيجيات الأمن الرقمي يؤثر إيجابًا في بعض النواحي على استخدامهم الفعلي لها، خاصة في استخدام الأدوات البسيطة مثل تغيير كلمات المرور واستخدام المصادقة الثنائية واستخدام أدوات مكافحة البرامج الضارة ومضادات الفيروسات، بينما لم تنعكس المعرفة بأدوات الأمان القوية كالتشفير على استخدامهم لها.

الفرض الثاني: توجد علاقة بين التحديات التي يواجهها الصحفيون وقد تقف عقبة أمام تحقيق أمنهم الرقمي، وبين استخدامهم لأدوات الأمن الرقمي.

		مقياس درجة الاستخدام
التحديات	معامل الارتباط	0.327
	مستوي الدلالة	0.000
	ن	137

تشير بيانات الجدول السابق إلى وجود علاقة ارتباط عكسية، بين التحديات التي يواجهها الصحفيون، وبين تبنيهم للإجراءات التي تعزز من أمنهم الرقمي، حيث بلغت قيمة معامل ارتباط بيرسون -0.327، وهي دالة عند مستوى معنوية 0.00، أي أنه كلما زادت درجة الشعور بوجود تحديات كان ذلك عقبة أمام استخدامهم لأدوات الأمن الرقمي.

وتتفق النتائج مع نتائج دراسة (Franziska Roesner, et al. 2015)، ودراسة (Olunifesi S. and Olawale O., 2017)، حيث كان الاعتماد المحدود على أدوات الأمان بسبب تحديات قابلية الاستخدام، وعدم امتلاك المهارات الخاصة بالأمن الرقمي المطلوبة للعمل في البيئة الرقمية.

الفرض الثالث: توجد فروق بين المبحوثين الذين تعرضوا لمخاطر رقمية والذين لم يتعرضوا لها وبين مستوى استخدامهم لأدوات الأمن الرقمي.

الاستخدام / المخاطر	الإجمالي		المتوسط الحسابي	الانحراف المعياري	درجات الحرية	ف	مستوى المعنوية
	ك	%					
التعرض للمخاطر الرقمية	30	21.9%	2.6667	0.47871	4132	4.167	0.003
عدم التعرض لمخاطر	107	78.1%	1.9489	0.55750			

تشير بيانات الجدول السابق إلى وجود فروق ذات دلالة بين المبحوثين في استخدامهم لأدوات الأمن الرقمي وفقا لتعرضهم المسبق لمخاطر رقمية حيث كانت قيمة ف 4.167 عند مستوى معنوية 0.003 وهي دالة إحصائيا، ويمكن تفسير هذه النتيجة في إطار استجابات المبحوثون حول طبيعة المخاطر الرقمية التي تعرضوا لها بالفعل والتي كانت متمثلة في اختراق حسابات مواقع التواصل الاجتماعي والبريد الإلكتروني وهي تمثل مخاطر متكررة يتم التعامل معها عبر إجراء تأمين الحساب سواء التغيير الدوري لكلمات المرور أو ربط البريد برقهم الهاتف أو المصادقة الثنائية أو اختيار كلمات مرور قوية.

وتتفق هذه النتائج مع نتائج دراسة (Mitchell A., et al., 2015) حيث يؤكد الغالبية العظمى من الصحفيين على أن فوائد الاتصالات الرقمية تفوق المخاطر.

الفرض الرابع: توجد فروق بين استخدام المبحوثين لأدوات الأمن الرقمي وفقا لمستوى الخبرة الرقمية لديهم.

الخبرات / الاستخدام	الإجمالي		المتوسط الحسابي	الانحراف المعياري	درجات الحرية	ف	مستوى المعنوية
	ك	%					
مبتدئ	50	36.5%	1.6467	0.81250	2134	2.962	0.022
متوسط	76	55.5%	1.8912	0.73319			
مرتفع	11	8%	1.7778	0.73208			

تشير البيانات إلى وجود فروق دالة إحصائيا بين المبحوثين في استخدامهم للأدوات الأمن الرقمي وفقا لمستوى الخبرة الرقمية لديهم حيث كانت قيمة ف 2.962 عند مستوى معنوية 0.022.

وتتفق هذه النتائج مع نتائج دراسة (Tsui L., and Francis L., 2019) التي ذهبت إلى أن الصحفيين ذوي العقلية الأمنية المتقدمة أكثر قدرة على التعلم المستمر وتجربة الأدوات والتقنيات التي يمكنهم استخدامها من أجل تعزيز الحماية الرقمية، وتتفق أيضا مع دراسة (McGregor and Watkins, 2016) التي ذهبت إلى أن الصحفيين لم يقوموا بالكثير لتغيير ممارساتهم في مجال أمن المعلومات أو الاتصالات بسبب عدم فهمهم لأنظمة الاتصالات التكنولوجية والأدوات الرقمية اللازمة.

أهم نتائج الدراسة:

1. فرضت التطورات التكنولوجية على الصحفيين مهارات عديدة، تحتم عليهم العمل عبر المنافذ الرقمية بأساليب تكنولوجية، سواء في جمع المعلومات والتحقق منها؛ أو التواصل مع المصادر والزملاء والمؤسسة الصحفية؛ أو طرق التخزين الإلكتروني، مما يجعل مجال الأمن الرقمي أحد المجالات الهامة في الممارسات الصحفية القائمة على التكنولوجيا والإنترنت، تنبغي العناية به؛ سواء من قبل المؤسسات الصحفية، أو من قبل الصحفيين أنفسهم، من أجل تحقيق بيئة عمل آمنة.

2. لم يكن غالبية الصحفيين على دراية بأدوات مثل تشفير البريد الإلكتروني والملفات، أو تشفير اتصالاتهم، ويظهر الاعتقاد في تحقيق الأمن من خلال الحفاظ على أجهزتهم خالية من الفيروسات، واستخدام كلمات مرور قوية، مما يدلل على الحاجة لتوسيع مفهوم الوعي بالتهديدات الرقمية والأمن الرقمي لديهم.

3. لدى الصحفيين مجموعة من المشكلات المتعلقة بالأمن الرقمي، والتي يشعرون أنها قد تمثل إعاقة لعملهم، تمثل أهمها في التشفير الآمن وتحقيق الأمن في الهواتف الذكية وتحقيق الأمن والخصوصية في مواقع التواصل الاجتماعي، حيث تعكس هذه النتيجة شعور القلق تجاه هذه المنصات والأجهزة الرقمية، التي أصبحت تتمتع بقدر كبير من الوصول إلى بيانات المستخدمين وملفاتهم، مما قد يشعرهم بالتهديد، وهو ما لا يستقيم مع حساسية مجال العمل الصحفي.

4. يعتقد الصحفيون أن بياناتهم معرضة للاختراق، وأن أكثر الجهات التي تمثل تهديدًا لأمنهم الرقمي هي الجهات القائمة على التطبيقات التي يقومون بتثبيتها على أجهزتهم، حيث تتطلب منحها أذونات للوصول إلى بياناتهم، وهو ما قد لا يلتفت إليه الصحفيون والأفراد عامة، حيث يغلب طابع الموافقة العمياء لهذه الأذونات، من أجل الاستمرار في تثبيت التطبيق واستخدامه، دون مراجعة سياسة الاستخدام، أو الإعدادات التي تفرضها التطبيقات بشكل تلقائي، والتي غالبًا ما تكون مرتبطة بإتاحة بيانات

المستخدمين.

5. ويغلب على الصحفيين الاعتقاد بأن عملهم الصحفي يمثل حساسية كبيرة بالنسبة إليهم، قد تجعلهم عرضة لاحتمال جمع البيانات حولهم، حيث أفاد (95.6 %) منهم بذلك.

6. يمثل تسريب البيانات الشخصية، والخوف من انتهاك الخصوصية، مثار القلق الأكبر لدى الصحفيين، حيث تعتبر خسارة سرية البيانات والتسريبات الإلكترونية من أكثر أنواع الحروب الإلكترونية شيوعًا، ونظرا لأن الصحفي منوط به حماية مصادره، كان أحد المخاوف لدى الصحفيين من تسريب البيانات هو حصول الأطراف الثالثة على بيانات الأشخاص الذين يتواصل معهم الصحفي.

7. المخاطر الرقمية المحتملة لم تقف في الأغلب كعقبة أمام استخدام الصحفي للوسائل الرقمية، حيث أفاد بذلك (71.3 %) منهم، مما يؤكد ضرورة رفع وعي الصحفيين تجاه تدعيم الأمن الرقمي، واعتماد إستراتيجيات تمكنهم من الاستفادة من منافع التكنولوجيا بصورة آمنة، مما يجعل التدريب على أهمية الأمن الرقمي حتميًا.

8. أغلب الصحفيين لم يحصلوا مسبقًا على دورات تدريبية خاصة بالأمن الرقمي، حيث أفاد بذلك (73 %) من العينة، وكانت المبادرة الشخصية عبر التعلم الذاتي هي المحرك والدافع لبعض الصحفيين نحو الاهتمام بمسألة الأمن الرقمي.

9. رغم أنه لم يكن للمؤسسات الصحفية دور فاعل في إمداد الصحفيين بالدورات التدريبية اللازمة، حيث أفاد حوالي 10 % من الصحفيين فقط بحصولهم على دورات تدريبية بواسطة مؤسستهم. فإن أغلب المؤسسات تتيح دعمًا فنيًا للصحفيين، مما قد يدلل على وعي المؤسسات الصحفية تجاه الاهتمام بالجانب التقني، لكنها بحاجة إلى توجيه أفضل، وترى الباحثة ضرورة تدعيم هذا الوعي بتثقيف الصحفيين بشكل مباشر حول مفهوم الأمن الرقمي وأدواته؛ من منطلق أنه لا يجب الانتظار حتى وقوع الأزمة، ومن منطلق ضرورة الاستخدام المسبق للأدوات التي تحمي بيانات وعمل

الصحفي، لا سيما وأن الدعم الأمني الذي أفاد الصحفيين بأن المؤسسة توفره يكون مرتبطًا تجاه عدم اختراق المؤسسة من الخارج، وتأمين أجهزة العمل عن طريق وضع كلمة مرور شخصية لكل جهاز، واستخدام جدار الحماية الناري Fire Wall، للحماية من المواقع غير الآمنة، وهي تعد إستراتيجيات بسيطة بحاجة لدعم أكبر.

10. يحدد بعض الصحفيين احتياجاتهم التدريبية في مجال الأمن الرقمي في: قدرتهم على تقييم المخاطر الرقمية المحتملة، وإدارة كلمات المرور، ومهارات الحفاظ على خصوصية الاتصالات، وكيفية تأمين الحسابات الشخصية، وسبل الحفاظ علي خصوصية الهواتف الذكية.

11. تغلب على الصحفيين معرفة الإجراءات البسيطة المتاحة المتعلقة بتعزيز الأمن الرقمي على معرفتهم بالإجراءات الأكثر دقة.

12. وتنعكس هذه المعرفة المتوسطة على الاستخدامات الفعلية التي ينتهجونها، حيث يفضل بعض الصحفيين في المقام الأول إستراتيجية الدفاع غير الرقمي؛ من خلال المقابلة وجهًا لوجه لتخفيف مخاطر تداول البيانات أو الاتصالات، أما الإستراتيجيات الرقمية فقد انعكست معرفتهم بهذه الأدوات على قدرتهم على استخدامها، ما يدلل على صدق المبحوثين، حيث كانت الأدوات التقليدية للحفاظ على الأمن الرقمي، مثل العناية باختيار كلمات المرور، واعتماد المصادقة الثنائية، واستخدام برامج مكافحة الفيروسات، في مقدمة الأدوات التي يعتمدون عليها، بينما قل اعتمادهم على الإجراءات الأكثر دقة والتي تحتاج إلى مزيد من الجهد لتعلمها وتنفيذها، مثل استخدام الشبكات الافتراضية أو التشفير، رغم أنها قد تقدم لهم حماية أعلى.

13. تعد أبرز التحديدات التي يرى الصحفيون أنها قد تقف عقبة أمام تحقيق أمنهم الرقمي معيار سهولة الاستخدام، بالإضافة إلى عدم شيوع استخدام الأدوات التي تتطلب استخدام الطرف الآخر لها من المصادر أو الزملاء.

توصيات الدراسة:

1. الاهتمام بالفرص والفوائد التي يوفرها الأمن الرقمي، فقد يواجه الجميع تهديدات رقمية، إلا أنه لا ينبغي الانتظار حتى وقوعها، (كما صورت إحدى الدراسات: لا يجب على الصحفيين الانتظار لتعلم كيفية استخدام القفل للدراجة حتى يتم سرقتها) (Tsui L., and Francis L., 2019).

2. تبني المؤسسات الصحفية للمبادرات والمبادئ التوجيهية في مجال الأمن الرقمي، والاعتماد عليها في تنظيم ورش عمل ودورات تدريبية للصحفيين.

3. تركيز تدريب الصحفيين على كيفية تحقيق أقصى درجات الأمان على هواتفهم الذكية، باعتبارها الوسيلة الأكثر استخدامها ولها خصائصها وميزاتها التي تنفرد بها عن أجهزة الحاسوب التي اعتاد الصحفيون على استخدامها سابقًا، بالإضافة إلى حساسية فقدها أو سرقتها.

4. إنشاء شبكة متخصصة للصحفيين، تدعم تقديم الأمن للصحفيين العاملين بشكل حر ولا يتبعون مؤسسات معينة.

5. تضمين الأمن الرقمي كوحدات دراسية في برامج الصحافة والإعلام بصفة عامة، واعتبار تثقيف الطلاب المقبلين على العمل الصحفي حاجة ملحة.

6. مشاركة أصحاب المصالح في دعم مبادرات نشر ثقافة الوعي بالأمن الرقمي، من أفراد ومؤسسات صحفية ونقابات ومنظمات غير حكومية.

7. تشجيع الشراكة مع المؤسسات التكنولوجية، من أجل زيادة الدعم التقني، وزيادة الموارد المخصصة للصحفيين للحفاظ على أمنهم الرقمي.

قائمة المراجع:

1- UNESCO, Model curricula for journalism education: a compendium of new syllabi, 2013, Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000221199.

2- International Research & Exchanges Board - IREX, SAFE Basic Training Curriculum for Media Practitioners and Social Communicators, Retrieved from: www.irex.org/resource/safe-basic-training-curriculum-media-practitioners-and-social-communicators.

3- www.cyber-arabs.com.

4- SKeyes Center for Media and Cultural Freedom, The Journalist Survival Guide, Retrieved from: video.skeyesmedia.org.

5- Internews, SaferJourno: Digital Security Resources for Media Trainers, Av Retrieved from: https://saferjourno.internews.org/.

6- Henrichsen, Jennifer R., Michelle Betz, and Joanne M. Lisosky. Building Digital Safety for Journalism: A Survey of Selected Issues. Op. Cit., PP. 39-40.

7-تتوفر الأدلة على موقع وزارة الاتصالات وتكنولوجيا المعلومات، ومنها
www.mcit.gov.eg/Ar/Publication/Publication_Summary/972,
www.mcit.gov.eg/Ar/Publication/Publication_Summary/618.

8- McGregor, Susan E., and Elizabeth Anne Watkins. "Security by Obscurity": Journalists' Mental Models of

Information Security." Quieting the Commenters: The Spiral of Silence's Persistent Effect (2016) PP. 34-37.

9- Greenwald, G. NSA collecting phone records of millions of Verizon customers daily. The Guardian 6 Jun 2013. Retrieved from www.theguardian.com/world/2013/jun/06/nsa-phone-recordsverizon-court-order.

10- James Ball, Bruce Schneier and Glenn Greenwald, NSA and GCHQ target Tor network that protects anonymity of web users, Retrieved from : www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

11- Greenwald, G. & MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian 7 Jun 2013. Retrieved from www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

12- McGregor, Susan E., and Elizabeth Anne Watkins. ""Security by Obscurity": Journalists' Mental Models of Information Security." Op. Cit..

13- Janet Reitman, Snowden and Greenwald: The Men Who Leaked the Secrets, Retrieved from: www.rollingstone.com/culture/culture-news/snowden-and-greenwald-the-men-who-leaked-the-secrets-104970/.

14- Lee, Micah, and Randi Heinrichs. "How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. An interview with Micah Lee." ephemera: theory & politics in organization 19.4 (2019) P. 811.

15- Papantoniou, Bill, et al. "The Glossary of Human

Computer Interaction." Online Retrieved from: www. interaction-design. org/literature/book/the-glossary-of-humancomputer-interaction (2016).

16- Johnson-Laird, Philip Nicholas. Mental models: Towards a cognitive science of language, inference, and consciousness. No. 6. Harvard University Press, (1983).

17- Bravo-Lillo, Cristian, et al. "Bridging the gap in computer security warnings: A mental model approach." IEEE Security & Privacy 9.2 (2010): 18-26.

18- McGregor, Susan E., and Elizabeth Anne Watkins. "Security by Obscurity": Journalists' Mental Models of Information Security." Quieting the Commenters: The Spiral of Silence's Persistent Effect (2016): 33. P. 36.

19- Norman, Donald A. "Some observations on mental models." Mental models. Psychology Press, 2014. 15-22.

20- Ibid.

21- McGregor, Susan E., and Elizabeth Anne Watkins. ""Security by Obscurity": Journalists' Mental Models of Information Security." Op. Cit..

22- Ibid.

23- Wash, Rick, and Emilee Rader. "Influencing mental models of security: a research agenda." Proceedings of the 2011 New Security Paradigms Workshop. 2011.

24- McGregor, Susan E., and Elizabeth Anne Watkins. ""Security by Obscurity": Journalists' Mental Models of Information Security." Op. Cit..

25- Ibid.

26- Wash, Rick. "Folk models of home computer security." Proceedings of the Sixth Symposium on Usable Privacy and Security. 2010.

27- Tsui, Lokman, and Francis Lee. "How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom." Journalism (2019): 1464884919849418. PP. 9-13.

28- Shere, Anjuli RK, Jason RC Nurse, and Ivan Flechais. "Security should be there by default: Investigating how journalists perceive and respond to risks from the Internet of Things." (2020).

29- Tsui, Lokman, and Francis Lee. "How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom." Journalism (2019), Op. Cit..

30- Çalışkan, Behlül. "Digital security awareness and practices of journalists in Turkey: A descriptive study." Conflict & Communication 18.1 (2019).

31- Lokman Tsui, The importance of digital security to securing press freedom. (Journalism, Vol. 20, No. 1, 2019), PP. 80–82. Retrieved from: https://doi.org/10.1177/1464884918809276.

32- Olunifesi Adekunle Suraj and Olawale Olaleye, Digital Safety among Nigerian Journalists, in: The Assault on Journalism, Edited by Ulla Carlsson and Reeta Pöyhtäri, Nordicom, Sweden, 2017, PP. 329 -333.

33- Javier Garza Ramos, Journalist Security in the Digital World: A Survey, Are We Using the Right Tools?, The Center

for International Media Assistance (CIMA), 2016, Retrieved from www.cima.ned.org/wp-content/uploads/2016/03/CIMA-Journalist-Digital-Tools-03-01-15.pdf.

34- McGregor, Susan E., and Elizabeth Anne Watkins. ""Security by Obscurity": Journalists' Mental Models of Information Security." Op. Cit.

35- Holcomb, Jesse, Amy Mitchell, and Kristen Purcell. "Investigative journalists and digital security." Pew Research Center. Retrieved from: www. journalism. org/2015/02/05/investigative-journalists-and-digital-security (2015).

36- Sierra, Jorge Luis. Digital and Mobile Security for Mexican Journalists and Bloggers: Results of a Survey of Mexican Journalists and Bloggers. Freedom House, 2013. Retrieval from: https://freedomhouse.org/report/special-reports/digital-and-mobile-security-mexican-journalists-and-bloggers.

37- Franziska Roesner, et al. "Investigating the computer security practices and needs of journalists." 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015. Retrieved from: www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf

38- SECONDMUSE. Information Security for Journalists, June 2014. Retrieved from: http://internetfreedom.secondmuse.com/wp-content/uploads/2015/08/if_vietnam_v1.1.pdf.

39- Internews Center for Innovation & Learning, Digital Security and Journalists, Pakistan 2012, A SnapShot of

Awareness and Practice in Pakistan. Retrieval from: www.internews.org/sites/default/files/resources/Internews_PK_Secure_Journalist_2012-08.pdf.

40- Ferrier, Michelle, and Nisha Garud-Patkar. "TrollBusters: Fighting online harassment of women journalists." Mediating Misogyny. Palgrave Macmillan, Cham, 2018. PP. 311-332.

41- Ron Deibert, digital threats against journalists. in: Journalism after Snowden: the future of the free press in the surveillance state. Edited by: Emily Bell, Taylor Owen, Smitha Khorana and Jennifer R. Henrichsen. Columbia University Press, 2017. PP. 240 -257.

42- McGregor, Susan E. "Digital Security and Source Protection for Journalists." (2014). Retrieval from: https://academiccommons.columbia.edu/doi/10.7916/D8611BRM/download.

43- Carlo, Silkie, and Arjen Kamphuis. "Information Security for Journalists." The Centre for Investigative Journalism, Jul (2014).

44- Internews, SaferJourno: Digital Security Resources for Media Trainers, Op. Cit.

45- IREX, SAFE Basic Training Curriculum for Media Practitioners and Social Communicators, Retrieved from: www.irex.org/resource/safe-basic-training-curriculum-media-practitioners-and-social-communicators.

46- Henrichsen, Jennifer R., Michelle Betz, and Joanne M. Lisosky. Building digital safety for journalism: A survey of selected issues. Op. Cit., 2015.

47- Lee, Micah. "Encryption works: How to protect your privacy in the age of NSA surveillance." Freedom of the Press Foundation (2013). Retrieved from: https://github.com/freedomofpress/encryption-works/blob/master/encryption_works.md

48- https://wickr.com.

49- https://signal.org.

50- https://guardianproject.info.

51- https://www.ccleaner.com/ccleaner.

52- http://truecrypt.sourceforge.net/.

53- https://www.torproject.org/.

54- https://tails.boum.org/.

55- Kashmir Hill, Lavabit's Ladar Levison: 'If You Knew What I Know About Email, You Might Not Use It', 2013, Retrieved from: www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/#25b464e0648a.

56 - Parmy Olson, E-mail's Big Privacy Problem: Q& A With Silent Circle Co-Founder Phil Zimmermann, 2013, Retrieved from: www.forbes.com/sites/parmyolson/2013/08/09/e-mails-big-privacy-problem-qa-with-silent-circle-co-founder-phil-zimmermann/#739203137403.

57- Norcie, Greg, et al. "Why Johnny can't blow the whistle: Identifying and reducing usability issues in anonymity systems." Proceedings 2014 Workshop on Usable Security. Retrieved from: https://doi. org/10.14722/usec. 2014.

58 - The Syria Justice and Accountability Centre (SJAC), Retrieved from: https://ar.syriaaccountability.org/database/.

59- Gaw, Shirley, Edward W. Felten, and Patricia Fernandez-Kelly. "Secrecy, flagging, and paranoia: adoption criteria in encrypted email." Proceedings of the SIGCHI conference on human factors in computing systems. 2006.

60- Rader, Emilee, and Rick Wash. "Identifying patterns in informal sources of security information." Journal of Cybersecurity 1.1 (2015): 121-144..

61- Wash, Rick, and Emilee Rader. "Influencing mental models of security: a research agenda." Op. Cit.

62- Asgharpour, Farzaneh, Debin Liu, and L. Jean Camp. "Mental Models of Computer Security Risks." WEIS. 2007..

63- Wash, Rick. "Folk models of home computer security." Op. Cit.

64- Kang, Ruogu, et al. ""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security." Eleventh Symposium On Usable Privacy and Security {SOUPS} 2015.

65- Kumar, Priya, et al. "'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online." Proceedings of the ACM on Human-Computer Interaction 1.CSCW (2017): PP.1-21.

66- Bravo-Lillo, Cristian, et al. "Bridging the gap in computer security warnings: A mental model approach." Op. Cit., PP.18-26.

67- Friedman, Batya, et al. "Users' conceptions of risks and harms on the web: a comparative study." CHI'02 extended abstracts on Human factors in computing systems. 2002.

68- Fulton, Kelsey R., et al. "The effect of entertainment media on mental models of computer security." Fifteenth Symposium on Usable Privacy and Security. 2019.

69- Redmiles, Elissa M., Amelia R. Malone, and Michelle L. Mazurek. "I think they're trying to tell me something: Advice sources and selection for digital security." 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.

70- Furnell S Moore L . Security literacy: the missing link in today's online society? Comput Fraud Secur Bull 2014 ; 2014. PP. 12 – 18 .

71- James, Tabitha, Quinton Nottingham, and Byung Cho Kim. "Determining the antecedents of digital security practices in the general public dimension." Information Technology and Management 14.2 2013: PP.69-89.

72- Furnell, Steve M., Peter Bryant, and Andrew D. Phippen. "Assessing the security perceptions of personal Internet users." Computers & Security 26.5 ,2007, PP. 410-417.

73- LaRose R Rifon NJ Enbody R . Promoting personal responsibility for internet safety . Commun ACM 2008 ; 51 : PP. 71 – 76 .

74 – أسماء المحكمين مرتبة هجائيا:

أ. د. آمال كمال، أستاذ الصحافة، قسم الإعلام، كلية الآداب، جامعة حلوان.

أ. د. حلمي محسب، أستاذ الصحافة، كلية الإعلام، جامعة جنوب الوادي.

أ. د. سحر فاروق، أستاذ الصحافة، قسم الإعلام، كلية الآداب، جامعة حلوان.

أ. د. شريف درويش اللبان، وكيل كلية الإعلام ، جامعة القاهرة.

أ. د. محمد سعد، عميد المعهد العالي للإعلام، أكاديمية الشروق.

75- Committed to connecting the world, Definition of cybersecurity. Retrieved from:

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

76- Hatleback, Eric N. "The protoscience of cybersecurity." The Journal of Defense Modeling and Simulation vol. 15, no. 1, Jan. 2018, P. 6.

77- Boyce, Michael W., et al. "Human performance in cybersecurity: A research agenda." Proceedings of the Human Factors and Ergonomics Society annual meeting. Vol. 55. No. 1. Sage CA: Los Angeles, CA: SAGE Publications, 2011.

78- Kaspersky, What is Cyber-Security?, Retrieved from: www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

79- Ron Deibert, digital threats against journalists. in: Journalism after Snowden: the future of the free press in the surveillance state. Edited by: Emily Bell, Taylor Owen, Smitha Khorana and Jennifer R. Henrichsen. Columbia University Press, 2017. PP. 240 : 257.

80- Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security 38, 2013. PP. 97-98.

81- Saltzstein, William. "Bluetooth Wireless Technology

Cybersecurity and Diabetes Technology Devices." Journal of diabetes science and technology (2019): 1932296819864416.

82- Kaspersky, What is Cyber-Security?, Op. Cit.

83 - تتوفر الاستراتيجية على موقع وزارة الاتصالات وتكنولوجيا المعلومات، www.mcit.gov.eg/

84- Pavlik, John V. "Transformation: examining the implications of emerging technology for journalism, media and society." Athens Journal of Mass Media and Communications 1.1 (2015): 19.

85- McGregor, Susan E., and Elizabeth Anne Watkins. ""Security by Obscurity": Journalists' Mental Models of Information Security." Quieting the Commenters: The Spiral of Silence's Persistent Effect (2016): 33. P. 37.

86- Kaspersky, What is Cyber-Security?, Op. Cit.

87- Di Salvo, Phillip. "Hacking/Journalism." limn (2017).

88- Mendel, Toby, et al. Global Survey on Internet Privacy and Freedom of Expression. UNESCO, 2012. P. 29 .

89- Pavlik, John V. "Transformation: examining the implications of emerging technology for journalism, media and society." Op. Cit., P. 11

90- Mendel, Toby, et al. Global Survey on Internet Privacy and Freedom of Expression. Op. Cit.

91- Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." IEEE Security & Privacy 8.6 (2010): P. 28.

92- Mendel, Toby, et al. Global Survey on Internet Privacy

and Freedom of Expression. Op. Cit.

93- Mats Sjöberg, Hung-Han Chen, Patrik Floréen, Markus Koskela, Kai Kuikkaniemi, Tuukka Lehtiniemi and Jaakko Peltonen, Digital Me: Controlling and Making Sense of My Digital Footprint. In: Symbiotic Interaction, 5th International Workshop, Symbiotic 2016, Springer, 2017, PP. 155-167.

94- Rory Peck guide, Digital Security Risk Assessment Guide, rorypecktrust.org.

95- Rodosek, Gabi Dreo, and Mario Golling. "Cyber security: challenges and application areas." Supply Chain Safety Management. Springer, Berlin, Heidelberg, 2013. P. 186.

96- Rory Peck guide, Digital Security Risk Assessment Guide, Op. Cit.

97- Javier Garza Ramos, Journalist Security in the Digital World: A Survey, Are We Using the Right Tools?, Op. Cit.

98- Mendel, Toby, et al. Global Survey on Internet Privacy and Freedom of Expression. Op. Cit.

99- Scott A. Golder and Michael W. Macy, Digital Footprints: Opportunities and Challenges for Online Social Research, (The Annual Review of Sociology, 2014), P. 132.

100- Bobbe Baggio and Yoany Beldarrain, "How Safe Is Your Identity? Security Threats, Data Mining, and Digital Fingerprints/Footprints. in: Cyber Crime : Concepts, Methodologies, Tools and Applications, eds: Information Science Publishing IGI Global, USA, 2012, P. 53.

101- Jordan Hitchcock, Public or private? A social cognitive exploratory study of privacy on social networking

sites, (MA. Thesis in Communication, California State University, Fullerton, 2008), P. 36, Available from ProQuest Dissertations & Theses Global. (304827494). Retrieved from http://proxy.binghamton.edu/login?url=https://search-proquest-com.proxy.binghamton.edu/docview/304827494?accountid=14168.

102- Kaspersky, What is Cyber-Security?, Op. Cit.

103- Pieter Arntz, Cybersecurity for journalists: How to defeat threat actors and defend freedom of the press, Retrieved from: https://blog.malwarebytes.com/how-tos-2/2019/11/cybersecurity-for-journalists-how-to-defeat-threat-actors-and-defend-freedom-of-the-press/.

104 - Rader, Emilee, and Rick Wash. "Identifying patterns in informal sources of security information." Op. Cit.

105- Shere, Anjuli RK, Jason RC Nurse, and Ivan Flechais. "Security should be there by default: Investigating how journalists perceive and respond to risks from the Internet of Things." Op. Cit. P. 8.

106 - Retrieved from:

- Andy Greenberg, These Are the Emails Snowden Sent to First Introduce His Epic NSA Leaks, 2014, www.wired.com/2014/10/snowdens-first-emails-to-poitras/.
- Peter Maass, How Laura Poitras Helped Snowden Spill His Secrets, 2013, www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html.
- Micah Lee, Ed Snowden Taught Me To Smuggle Secrets Past Incredible Danger. Now I Teach You. 2014,

https://theintercept.com/2014/10/28/smuggling-snowden-secrets/..

107 - Yar, Majid. "Computer hacking: Just another case of juvenile delinquency?." The Howard Journal of Criminal Justice 44.4 2005, PP. 387-399.