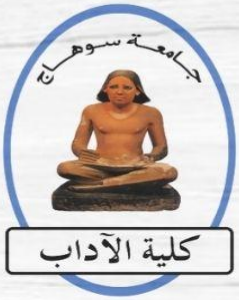

المجلة المصرية لبحوث الاتصال والإعلام الرقمي

مجلة دورية محكمة تصدر عن قسم الإعلام بكلية الآداب - جامعة سوهاج

المجلد 5 العدد 5

Issn: 3009-7134

https://ejrcds.journals.ekb.eg

يناير - 2025

الفهرست:

الأمن السيبراني في غرف الأخبار الصحفية: استراتيجيات وتحديات

المؤلف: أحمد جعفر أحمد محمد ✉

Doi: https://doi.org/10.21608/ejcrds.2024.321185.1022

الملخص:

تهدف الدراسة إلى استكشاف التحديات الأمنية التي تواجه غرف الأخبار في العصر الرقمي، ورصد أنواع الهجمات الإلكترونية التي تتعرض لها، مع اقتراح حلول لتعزيز الأمن السيبراني. وتعتمد الدراسة على منهج المسح الإعلامي، لجمع البيانات من عينة من الصحفيين والعاملين في غرف الأخبار في مصر، باستخدام استبيان إلكتروني.

وتوصلت الدراسة إلى عدة توصيات وهي: ينبغي على غرف الأخبار أن تتبنى نهجًا متعدد الأبعاد لتعزيز أمنها السيبراني . ويجب أن يشمل هذا النهج توفير تدريب مستمر وشامل للعاملين، ليس فقط على التعرف على التهديدات السيبرانية، ولكن أيضًا على أفضل الممارسات الأمنية وكيفية التصرف في حالة وقوع هجوم. علاوة على ذلك، ينبغي نشر الوعي بأهمية الأمن السيبراني من خلال حملات توعية داخلية، ودورات تدريبية.

وعلى الصعيد التقني، يجب الحرص على تحديث جميع البرامج وأنظمة التشغيل المستخدمة في غرف الأخبار بشكل دوري، وتثبيت وتحديث برامج مكافحة الفيروسات وجدران الحماية على جميع الأجهزة. بالإضافة إلى ذلك، ينبغي استخدام كلمات مرور قوية وفريدة من نوعها لكل حساب، وتغييرها بشكل دوري، واستخدام التشفير لحماية البيانات الحساسة، وإجراء نسخ احتياطي منتظم للبيانات الهامة وتخزينها في مكان آمن. وهذا لجعل غرف الاخبار أكثر أماناً سيبرانياً.

ويجب على غرف الأخبار بناء علاقات تعاون مع الجهات الأمنية المختصة، والمشاركة في المبادرات والفعاليات التي تهدف إلى تعزيز الأمن السيبراني في قطاع الإعلام. والأهم من ذلك كله، يجب العمل على بناء ثقافة أمنية قوية داخل غرفة الأخبار، حيث يشعر الجميع بالمسؤولية تجاه الأمن السيبراني، ويتم تشجيع الإبلاغ عن أي حوادث محتملة دون خوف من العقاب.

الكلمات المفتاحية: الأمن السيبراني، غرف الأخبار، الأمن الإلكتروني، الجرائم الإلكترونية

مقدمة:

أصبحت غرف الأخبار ساحة معركة جديدة في حرب المعلومات. فلم تعد التهديدات الأمنية مقتصرة على العالم المادي، بل امتدت إلى الفضاء الإلكتروني، مهددةً عمل الصحفيين وسلامة المؤسسات الإعلامي؛ حيث تشير الإحصائيات إلى تصاعد حدة هذه التهديدات، ففي كل 10 ثوانٍ تحدث جريمة إلكترونية جديدة، وتتعرض المؤسسات والشركات لأكثر من 2000 هجمة يومياً. حتى الهواتف الذكية، التي أصبحت أداة أساسية للصحفيين، ليست بمنأى عن الخطر، حيث يحمل واحد من كل 36 هاتف أندرويد تطبيقات قد تعرض بيانات المستخدمين للخطر.

ولعل أبرز دليل على خطورة الوضع هو الهجمات المتكررة التي استهدفت مؤسسات إعلامية مرموقة حول العالم، مثل "نيويورك تايمز" و"شارلي إبدو" و"الأهرام." حيث تسببت هذه الهجمات في تعطيل العمل، وتسريب معلومات حساسة، وحتى تهديد حياة الصحفيين.

وفي ظل هذا الواقع المقلق، يصبح الأمن الإلكتروني في غرف الأخبار بالمؤسسات الصحفية ليس مجرد خيار، بل ضرورة حتمية. ويتعين على المؤسسات الإعلامية تبني استراتيجيات استباقية لحماية أنظمتها وبياناتها، وتدريب صحفييها على أفضل الممارسات الأمنية.

وبما إن التحديات كبيرة، لكن الفرص أيضاً متاحة. فمن خلال التوعية والتدريب، وتحديث الأنظمة، واستخدام التقنيات الحديثة، يمكن لغرف الأخبار أن تحمي نفسها من الهجمات الإلكترونية، وتحافظ على استقلاليتها وسلامة صحفييها، وتستمر في أداء رسالتها الإعلامية بكل حرية ومسؤولية.

ومما تقدم يتبين أهمية الوعي بالجرائم الإلكترونية وسبل مكافحتها من جانب الصحفيين المصريين بشكل خاص، ونتيجة لغياب هذا الوعي أو انخفاض مستواه تعرضت الكثير من المؤسسات الصحفية والإعلامية إلى بعض أنواع الجرائم الإلكترونية، ومن هنا تأتي أهمية دراسة الوقوف على مستويات الوعي بالأمن السيبراني بغرف الأخبار وسبل تفعيله وكيفية مواجهة الجرائم الإلكترونية ومكافحتها في المؤسسات الصحفية والإعلامية وخاصة في الدول النامية.

الدراسات السابقة:

من خلال التعرض لعدد من الدراسات السابقة في هذا الحقل البحثي نجد في **دراسة (Crete ,2020)** "ثقافة أمن المعلومات بالمؤسسات الصحفية الكندية، وأثرها على الصحفيين"، أنه تم التركيز على فهم مستوى وعي الصحفيين بأهمية أمن المعلومات، ودور المؤسسات الصحفية في تعزيز هذا الوعي.

وأظهرت الدراسة أن الصحفيين الاستقصائيين الذين يغطون قضايا حساسة يدركون أهمية أمن المعلومات، في حين يعتبره المراسلون الذين يغطون مواضيع أقل حساسية أمرًا ثانويًا .كما أكدت الدراسة على أن حماية المصدر تعتبر التزامًا مهنيًا أساسيًا للصحفيين الاستقصائيين، وأن هناك حاجة إلى تطبيق أساليب محددة لتعزيز ثقافة أمن المعلومات على المستويين المهني والمؤسسي. بالإضافة إلى ذلك، أشارت الدراسة إلى أن تعزيز الأمن الرقمي للصحفيين يساهم في إنتاج تقارير أكثر أمانًا وجودة، وأنه يجب على المؤسسات الصحفية توفير الوعي والمهارات الأساسية لأمن المعلومات لجميع الصحفيين، بغض النظر عن مناصبهم. (Crete ,2020)

أما في دراسة **وسام محمد أحمد (2020)** بعنوان "إدراك الصحفيين للمخاطر الرقمية وإستراتيجيات تطبيقهم للأمن الرقمي في عملهم المهني"، تم تسليط الضوء على أهمية الأمن الرقمي للصحفيين المصريين في ظل التطورات التكنولوجية المتسارعة.

وأكدت الدراسة أن التكنولوجيا الحديثة تتطلب من الصحفيين اكتساب مهارات تقنية جديدة، مما يجعل الأمن الرقمي ضرورة لا غنى عنها في بيئة العمل الصحفية المعتمدة على الإنترنت .وأشارت إلى أن معظم الصحفيين يدركون أنهم عرضة للهجمات الرقمية، ولكنهم يفتقرون إلى المعرفة بأدوات الأمن الرقمي، مما يؤكد الحاجة إلى زيادة الوعي في هذا المجال. وكشفت الدراسة أيضًا أن غالبية الصحفيين لم يتلقوا أي تدريب رسمي على الأمن الرقمي، وأنهم يعتمدون بشكل أساسي على التعلم الذاتي لزيادة وعيهم .وأعربوا عن رغبتهم في أن تتبنى مؤسساتهم الإعلامية برامج تدريبية لتعزيز مهاراتهم في هذا المجال. وأخيرًا، أظهرت الدراسة أن مخاوف الصحفيين الرئيسية تتعلق بتسريب البيانات الشخصية، وانتهاك الخصوصية، وفقدان البيانات، بالإضافة إلى القلق على سلامة مصادرهم وبياناتهم الشخصية عند استخدام تطبيقات الهاتف المحمول. (أحمد، 2020)

وفي دراسة **نرمين نبيل الأزرق (2020)** بعنوان "التهديدات الرقمية ضد الصحفيين المصريين ووعيهم بالآليات المستخدمة للحفاظ على سلامتهم"، تم تسليط الضوء على وعي الصحفيين المصريين بالمخاطر الرقمية التي يتعرضون لها، وكيفية تعاملهم مع هذه التهديدات.

وأظهرت الدراسة أن الصحفيين يعتمدون بشكل كبير على الإنترنت في عملهم، وأنهم يدركون المخاطر المحتملة . وقد حددوا مجموعة متنوعة من التهديدات الرقمية، بما في ذلك التسريبات، ونشر الشائعات، وحملات التشهير، وانتهاك الخصوصية، والتصيد الاحتيالي، والمراقبة، والقرصنة، والبرامج الضارة، والتضليل، والتحرش الجنسي عبر الإنترنت. ومع ذلك، كشفت الدراسة أن نسبة قليلة فقط من الصحفيين يعرفون كيفية حماية أنفسهم بشكل فعال من هذه التهديدات، وأن معظمهم يفتقرون إلى المعرفة بأدوات وتقنيات الأمن الرقمي .ويعزو الصحفيون ذلك إلى عدم وجود تدريب كافٍ في هذا المجال. بالإضافة إلى ذلك، يعتقد معظم الصحفيين أن الإطار

القانوني الحالي في مصر بحاجة إلى تطوير ليكون أكثر فعالية في مكافحة التهديدات الرقمية، وأن سياسات مؤسساتهم الإعلامية ليست كافية لحمايتهم .ويرى الصحفيون أنهم بحاجة إلى تدريب مهني متخصص لزيادة وعيهم بالتهديدات الرقمية وتزويدهم بالمهارات اللازمة لمواجهتها. (الأزرق، 2020)

وفي دراسة تشين (2020)، "التهديدات الرقمية التي يتعرض لها الصحفيون، واستراتيجيات الحماية منها"، تم تسليط الضوء على العلاقة بين وعي الصحفيين بالأمن الرقمي واستخدامهم لأدوات الحماية، بالإضافة إلى التحديات التي تواجههم في هذا المجال.

وأظهرت الدراسة أن الصحفيين الذين يغطون موضوعات حساسة هم أكثر استخدامًا للحماية الرقمية، وأن المهارات التقنية تلعب دورًا هامًا في تكرار استخدام هذه الأدوات .ومع ذلك، فإن غالبية الصحفيين يفتقرون إلى المهارات التقنية اللازمة، مما يجعلهم أكثر عرضة للمخاطر الإلكترونية. بالإضافة إلى ذلك، كشفت الدراسة عن عدة تحديات تعوق استخدام الحماية الرقمية، بما في ذلك قلة الوعي بالأمن السيبراني، والافتقار إلى المهارات التقنية، ومحدودية التدريب .وهذه التحديات تزيد من احتمالية تعرض الصحفيين للمراقبة والهجمات الضارة. وأخيرًا، أشارت الدراسة إلى أن استخدام الصحفيين لأدوات الحماية الرقمية يتأثر بعدة عوامل، منها نوع المحتوى الإخباري الذي يغطونه، والوسائط الرقمية التي يستخدمونها، ومناصبهم في غرف الأخبار، ومهاراتهم الفنية، ومنطقة عملهم، وجنسهم، وعملهم في الصحف الإلكترونية. (Chen, 2020)

وفي دراسة شيري (2020)، "إدراك الصحفيين بمخاطر وتهديدات إنترنت الأشياء، وردود فعلهم نحوها"، تم الكشف عن المخاطر الإلكترونية التي يواجهها الصحفيون واستراتيجياتهم للتعامل معها.

وأبرزت الدراسة أن أخطر التهديدات التي تواجه الصحفيين هي تهديد سرية المعلومات وسلامتها وتوافرها، بالإضافة إلى المراقبة الإلكترونية والتجسس .وقد أشار الصحفيون إلى أن معظم زملائهم يفتقرون إلى الوعي الكافي بمخاطر الأمن المعلوماتي، وأنهم لا يتخذون إجراءات وقائية مسبقة، بل يميلون إلى طلب المساعدة فقط بعد التعرض للهجوم. ومن بين أساليب الحماية التي اقترحها الصحفيون :تقليل التفاعل مع الأجهزة الإلكترونية، والاعتماد على طرق الاتصال التقليدية، وتعطيل التطبيقات عند عدم استخدامها، واستخدام آليات الاتصال المشفرة، وتجنب تخزين المعلومات الحساسة رقميًا، وتجنب استخدام البريد الإلكتروني في القضايا الحساسة، وتعزيز كلمات المرور، واستخدام جدار الحماية، وتجنب شبكات الواي فاي العامة، وتوفير التدريب الأمني للصحفيين، وسن تشريعات للحماية الرقمية. (Shere, 2020)

وفي دراسة (Christofoletti ,2018)، بعنوان "الهجمات والتهديدات الرقمية وانعكاساتها كمخاطر مهنية لدى الصحفيين"، تم تسليط الضوء على المخاطر الرقمية التي يتعرض لها الصحفيون وكيف تؤثر على عملهم.

وأظهرت الدراسة أن الصحفيين يواجهون صعوبة في فهم المخاطر الرقمية بسبب تعقيد مفاهيم الأمن الإلكتروني والمعلوماتي .كما بينت أن التكنولوجيا الحديثة زادت من تعقيد أمن وحرية الصحفيين، وأن المخاطر الرقمية يمكن اعتبارها شكلاً من أشكال العنف ضد الصحفيين، مما يؤثر على جودة المعلومات وسلامتها. وأوضحت الدراسة أيضًا أن الهجمات الإلكترونية التي تستهدف الصحفيين تهدف إلى التجسس، والتضليل، والتدمير، والكشف غير

المصرح به عن معلوماتهم الحساسة، مما قد يؤدي إلى مخاطر جسدية أو أضرار معنوية أو مادية .وأكدت أن هذه المخاطر هي نتيجة مباشرة لاستخدام الصحفيين لتكنولوجيا المعلومات والاتصال في عملهم اليومي. ومن بين الجرائم الإلكترونية التي تم تحديدها في الدراسة :مراقبة الموقع الجغرافي، واعتراض الرسائل، وتهديدات البريد الإلكتروني، وتثبيت فيروسات وبرامج خبيثة، واختراق الحسابات الشخصية، وسرقة كلمات المرور، وفقدان المعلومات، والتنصت على الهاتف. (Christofoletti ,2018)

وفي دراسة "المراقبة الرقمية للصحفيين بالولايات المتحدة وآثارها على علاقتهم بالمصدر" **لـ (2018 ,Waters)** تم تسليط الضوء على تأثير المراقبة الرقمية على عمل الصحفيين وعلاقتهم بمصادرهم.

وأشارت الدراسة إلى أن الصحفيين يجدون صعوبة في استخدام أدوات الأمن الرقمي للتواصل الآمن مع مصادرهم، ويفضل بعضهم اللقاءات المباشرة لتجنب المراقبة الإلكترونية .كما كشفت الدراسة عن أساليب الحماية التي يتبعها الصحفيون لحماية بياناتهم، مثل تجنب تخزين المعلومات الحساسة على الإنترنت وتجنب التواصل مع المصادر عبر وسائل التواصل الاجتماعي. وعلى الرغم من أن الصحفيين المشاركين في الدراسة لم يقدموا أدلة مباشرة على تعرضهم للمراقبة، إلا أنهم يعتقدون أن هناك احتمالًا لمراقبة اتصالاتهم المهنية .ويبذل الصحفيون جهودًا لتأمين اتصالاتهم والتهرب من المراقبة، إما باستخدام أدوات الأمن الرقمي أو بتجنب الاتصالات الرقمية تمامًا، لأنهم يرون أن المراقبة تعيق أداءهم المهني. (Waters, 2018)

وفي دراسة (McGregor, 2017)، بعنوان "تأثر الأمن الرقمي والخصوصية على ممارسات الصحفيين بغرف الأخبار بالولايات المتحدة الأمريكية"، تم استكشاف تأثير المخاوف الأمنية على سلوكيات الصحفيين أثناء جمع الأخبار وإنتاجها.

وأظهرت الدراسة أن الصحفيين يستخدمون قنوات اتصال مشفرة عند التواصل مع المصادر، ويفضلون الاتصال الهاتفي أو المقابلات الشخصية في حالة المعلومات الحساسة .كما أشارت الدراسة إلى أن الصحفيين يتخذون استراتيجيات مختلفة لزيادة خصوصيتهم وحماية أمنهم الرقمي، مثل تجنب الاتصالات القابلة للكشف، وممارسة الرقابة الذاتية على سلوكياتهم الرقمية. بالإضافة إلى ذلك، كشفت الدراسة عن مخاوف الصحفيين الشديدة تجاه الأمان والخصوصية والمراقبة، وعن فهمهم الجيد للأمن الإلكتروني والتهديدات الرقمية .وأكدت على أهمية تعاون الصحفيين في حماية المعلومات ورفع مهاراتهم التقنية. (McGregor, 2017)

وفي دراسة (Lundberg, 2017)، بعنوان "الأمن الرقمي للصحفيين السويديين ودوره في حماية المصدر"، تم استكشاف وعي الصحفيين السويديين بأهمية الأمن الرقمي وحماية المصدر، بالإضافة إلى التحديات التي تواجههم في هذا المجال.

وأظهرت الدراسة أن الصحفيين يتمتعون بوعي جيد فيما يتعلق بالأمن الرقمي، وأنهم يستخدمون أساليب وتقنيات مختلفة لحماية أنفسهم من الجرائم الإلكترونية، مثل استخدام البريد الإلكتروني المشفر والمكالمات المشفرة .ومع ذلك، يختلف مستوى الوعي والاهتمام بالأمن الرقمي من صحفي إلى آخر. وأعرب العديد من الصحفيين عن ثقتهم في التدابير الأمنية التي تتخذها مؤسساتهم، ولكنهم أكدوا على أهمية توفير أدوات اتصال سهلة الاستخدام

وغير معقدة. وأخيرًا، شددت الدراسة على أهمية توعية المصادر بأهمية الأمن الرقمي، حيث أن بعض المصادر قد لا تدرك المخاطر الإلكترونية التي قد يتعرضون لها، مما يعرضهم و الصحفيين للخطر. (Lundberg , 2017)

وفي دراسة (Caine ,2016)، بعنوان "واقع أمن الكمبيوتر وتهديدات الخصوصية الرقمية للمؤسسات الصحفية والصحفيين بالولايات المتحدة الأمريكية"، تم استكشاف وعي الصحفيين بأهمية الأمن الإلكتروني ودوافعهم لتبني استراتيجيات الحماية الرقمية.

وأكدت الدراسة أن الصحفيين يعتبرون حماية المصدر وسمعتهم من التهديدات الإلكترونية أولوية قصوى، حتى لو كان ذلك يعني التضحية بسهولة استخدام التقنيات التكنولوجية .ويركز الصحفيون على حماية مصادرهم وملفاتهم ومعلوماتهم الحساسة من الاختراق، لأن إفشاء هذه المعلومات يمكن أن يضر بسمعتهم وسمعة مؤسساتهم ويؤدي إلى فقدان الثقة والمصداقية. وأخيرًا، أشارت الدراسة إلى أن الصحفيين غالبًا ما يضطرون إلى التخلي عن بعض مبادئ الأمن الإلكتروني لتلبية متطلبات المصادر في اختيار طرق الاتصال، مما يعرضهم لمخاطر أمنية محتملة. (Caine ,2016)

وفي دراسة (Milosavljević ,2015)، بعنوان "اعتماد الصحفيين على الأمن الإلكتروني لتحقيق الاتصال الآمن بالمصدر"، تم تسليط الضوء على التحديات التي يواجهها الصحفيون في سلوفينيا بسبب تزايد المراقبة والتجسس الإلكتروني.

وأظهرت الدراسة أن الصحفيين يعتبرون أساليب المراقبة الجديدة تهديدًا حقيقيًا لعملهم، وأنهم قلقون بشأن إمكانية استخدام هذه الأساليب للتحكم في عملهم وتعقب مصادرهم .وقد أبلغ بعض الصحفيين عن شكوكهم في تعرضهم للمراقبة من قبل جهات حكومية أو خاصة. ومن المثير للقلق أن الدراسة كشفت عن عدم وجود سياسات أمنية أو تدابير محددة في المؤسسات الإعلامية السلوفانية لحماية الصحفيين ومصادرهم من المراقبة الإلكترونية، وأن الصحفيين أنفسهم يفتقرون إلى التدريب الأمني اللازم. وعلى الرغم من وعي الصحفيين بمسائل الأمن الإلكتروني والمراقبة المحتملة، إلا أن عدم وجود استجابة رسمية من مؤسساتهم الإعلامية يشير إلى بطء الاستجابة وقلة الوعي بهذه القضايا .والأكثر إثارة للقلق هو أن معظم الصحفيين المشاركين في الدراسة لا يرون حاجة لحماية معلوماتهم أو مصادرهم، وأن واحدًا منهم فقط يستخدم تطبيقات الأمان لتشفير اتصالاته وحماية جهازه من الاختراق. (Milosavljević ,2015)

وفي دراسة (Roesner , 2015)، بعنوان "احتياجات الصحفيين للأمن الرقمي وعلاقته بممارساتهم"، تم تسليط الضوء على التحديات التي يواجهها الصحفيون في تحقيق التوازن بين سهولة استخدام التقنيات التكنولوجية وأهمية الأمن الرقمي.

وأظهرت الدراسة أن الصحفيين يميلون إلى تفضيل سهولة استخدام أدوات الاتصال على حساب أمانها، مما يجعلهم عرضة للمخاطر الأمنية .كما أشارت الدراسة إلى أن استراتيجيات الأمن الإلكتروني قد تعرقل ممارسات الصحفيين اليومية وتبطئ من وتيرة عملهم، بالإضافة إلى أن نقص الأدوات التكنولوجية والدعم التقني يزيد من

التحديات الأمنية التي يواجهونها. ومن المثير للاهتمام أن الدراسة كشفت عن دور المؤسسات الإعلامية في تعزيز أو إعاقة تبني الصحفيين لأفكار الأمن الإلكتروني .ففي حين أن المؤسسة تلعب دورًا حاسمًا في نجاح وكفاءة أمن المعلومات، إلا أن تقييد صلاحيات الصحفيين في استخدام تطبيقات الأمان على أجهزتهم قد يقلل من اهتمامهم بالأمن الرقمي. (Roesner , 2015)

وفي دراسة (Mitchell, 2015)، بعنوان "الصحفيون الاستقصائيون وإدراكهم للأمن الرقمي، وعلاقته بتغيير أدائهم المهني"، تم تسليط الضوء على مخاوف الصحفيين من التهديدات الإلكترونية وتأثير ذلك على عملهم.

وأظهرت الدراسة أن نسبة كبيرة من الصحفيين يعتقدون أن الحكومة الأمريكية تجمع بيانات عن اتصالاتهم، وأن هذه المخاوف قد أثرت على تغطيتهم الصحفية وحتى دفعت بعضهم إلى ترك مجال الصحافة الاستقصائية .كما أشارت الدراسة إلى أن العديد من الصحفيين يرون أن مؤسساتهم لا تتخذ إجراءات كافية لحمايتهم من التهديدات الإلكترونية، وأنهم لم يتلقوا تدريبًا كافيًا في هذا المجال. وعلى الرغم من هذه المخاوف، يتخذ الصحفيون استراتيجيات مختلفة لحماية أنفسهم، مثل استخدام كلمات مرور قوية وتشديد إعدادات الخصوصية وإغلاق ميزة تتبع الموقع الجغرافي .ويرى معظمهم أن فوائد الاتصالات الرقمية تفوق مخاطرها، حيث تسهل هذه التقنيات أداءهم المهني وتجعله أكثر سرعة وفعالية. (Mitchell, 2015)

وفي دراسة أجراها INTERNEWS CENTER عام 2012 بعنوان "وعي الصحفيين بباكستان بالأمن الرقمي وانعكاسه على الأداء المهني"، تم تسليط الضوء على أولويات الصحفيين الباكستانيين عند استخدامهم للإنترنت ووسائل التواصل الاجتماعي، بالإضافة إلى التحديات التي يواجهونها في مجال الأمن الرقمي.

وكشفت الدراسة أن سهولة الاستخدام وشعبية منصات التواصل الاجتماعي تأتي في مقدمة أولويات الصحفيين، بينما يأتي الأمن والخصوصية في مرتبة متأخرة .وأشارت إلى أن نسبة قليلة فقط من الصحفيين يعتبرون الأمن أولوية قصوى عند استخدام هذه المنصات. وعلى الرغم من أن أكثر من نصف الصحفيين يهتمون بالحفاظ على سلامتهم أثناء استخدام الإنترنت، إلا أن الغالبية العظمى منهم لم يتلقوا أي تدريب على الأمن الرقمي .وأعرب الصحفيون عن قلقهم إزاء غياب قوانين جرائم الإنترنت في باكستان، وتأثير ذلك على عملهم اليومي .كما أشاروا إلى أن بعض أدوات الأمان المتقدمة معقدة وصعبة الاستخدام، مما يجعلهم يتجنبونها. (INTERNEWS ,2012 CENTER)

التعليق على الدراسات السابقة:

تستهدف الدراسات السابقة بشكل أساسي تحقيق فهم أعمق لتحديات الأمن الإلكتروني التي تواجه الصحفيين في العصر الرقمي. تسعى هذه الدراسات إلى تقييم وعي الصحفيين بأهمية الأمن الإلكتروني، ومدى استخدامهم لأدوات وتقنيات الحماية، بالإضافة إلى تحديد التهديدات الرقمية الأكثر شيوعًا التي يتعرضون لها. كما تهدف إلى دراسة تأثير المخاوف الأمنية على ممارساتهم وسلوكياتهم، وتقييم دور المؤسسات الإعلامية في تعزيز الأمن الرقمي. علاوة على ذلك، تستكشف هذه الدراسات العلاقة بين الأمن الرقمي وحرية الصحافة، وتسعى إلى إيجاد

توازن بينهما، وتقديم استراتيجيات وحلول عملية لتعزيز الأمن الرقمي للصحفيين وتمكينهم من حماية أنفسهم ومصادرهم ومعلوماتهم.

وتسلط الدراسات السابقة الضوء على مجموعة من النقاط الهامة المتعلقة بالأمن الإلكتروني للصحفيين:

- يختلف مستوى وعي الصحفيين بأهمية الأمن الإلكتروني تبعاً لنوعية عملهم وموضوعات تغطيتهم . الصحفيون الاستقصائيون الذين يتعاملون مع معلومات حساسة يبدون وعياً أكبر بأهمية الأمن الإلكتروني مقارنة بالصحفيين الذين يغطون موضوعات أقل حساسية.
- أظهرت العديد من الدراسات أن الصحفيين يفتقرون إلى المعرفة والمهارات اللازمة لاستخدام أدوات وتقنيات الأمن الرقمي بشكل فعال، مما يجعلهم أكثر عرضة للهجمات الإلكترونية.
- يفتقر العديد من الصحفيين إلى التدريب الرسمي على الأمن الإلكتروني، ويعتمدون بشكل أساسي على التعلم الذاتي . كما أن بعض المؤسسات الإعلامية لا توفر سياسات أمنية كافية أو تدابير لحماية صحفييها.
- تشمل مخاوف الصحفيين الرئيسية تسريب البيانات الشخصية، وانتهاك الخصوصية، والمراقبة الإلكترونية، والتجسس، والهجمات الضارة .هذه المخاوف قد تؤثر على أدائهم المهني وتدفعهم إلى تغيير سلوكياتهم أو حتى ترك مجال الصحافة الاستقصائية.
- يميل الصحفيون إلى تفضيل سهولة استخدام الأدوات التكنولوجية على حساب أمانها، وقد يجدون أن بعض أدوات الأمان معقدة وصعبة الاستخدام.
- يعتبر الصحفيون حماية مصادرهم من التهديدات الإلكترونية أولوية قصوى، وقد يتخذون إجراءات إضافية لتأمين اتصالاتهم مع المصادر.
- يرى بعض الصحفيين أن الإطار القانوني الحالي في بعض الدول بحاجة إلى تطوير ليكون أكثر فعالية في مكافحة التهديدات الرقمية وحماية الصحفيين.

مشكلة الدراسة:

على الرغم من الأهمية المتزايدة للأمن السيبراني في العصر الرقمي، إلا أن غرف الأخبار تواجه تحديات أمنية متصاعدة تهدد سلامة عملياتها وبياناتها وحتى سلامة الصحفيين أنفسهم .تشمل هذه التحديات الهجمات الإلكترونية المتنوعة، مثل الاختراق، والتجسس، وسرقة البيانات، والابتزاز، والتشهير، والتي تستهدف الصحفيين والمؤسسات الإعلامية على حد سواء.

وقد كشفت الدراسات السابقة عن فجوة كبيرة في فهم الصحفيين لهذه التهديدات، وافتقارهم إلى المهارات والمعرفة اللازمة للتعامل معها بشكل فعال .كما أشارت إلى قصور التشريعات والقوانين في مواكبة التطور السريع للجرائم الإلكترونية، مما يزيد من صعوبة مكافحتها وحماية المؤسسات الإعلامية.

وتسلط هذه الفجوة البحثية الضوء على ضرورة إجراء دراسة متعمقة للأمن السيبراني في غرف الأخبار، تهدف إلى استكشاف التحديات الأمنية المتنوعة التي تواجهها، وتأثيرها على سير العمل الصحفي، وتقييم مستوى الوعي

لدى العاملين والمؤسسات الإعلامية بهذه التحديات. كما تسعى الدراسة إلى استكشاف الاستراتيجيات والحلول العملية لتعزيز الأمن السيبراني في غرف الأخبار، بما يمكن الصحفيين من حماية أنفسهم ومصادرهم ومعلوماتهم، وضمان استمرارهم في أداء رسالتهم الإعلامية بحرية ومسؤولية في مواجهة التهديدات الإلكترونية المتزايدة.

أهمية الدراسة:

1. تمكين غرف الأخبار من مواجهة التحديات الأمنية وتزويد العاملين في غرف الأخبار بالوعي والمعرفة اللازمة للتعامل مع التهديدات السيبرانية المتزايدة، وتجنب الوقوع ضحية للهجمات الإلكترونية، مما يساهم في حماية عملياتهم وبياناتهم وسلامتهم، ويضمن استمرارية العمل الصحفي بكفاءة وفعالية.
2. مواكبة الاهتمام العالمي بتسليط الضوء على أهمية الأمن السيبراني للصحفيين، بما يتماشى مع التوجهات العالمية والاهتمام المتزايد من قبل المنظمات الصحفية العالمية ومنظمات حقوق الإنسان بمدى خطورة الهجمات الإلكترونية على حرية التعبير والعمل الصحفي.
3. دعم المؤسسات الإعلامية من خلال تقديم توصيات عملية للمؤسسات الإعلامية ونقابات الصحفيين وهيئات الإعلام لتعزيز الأمن السيبراني في غرف الأخبار، وتوفير بيئة عمل آمنة ومستقرة للصحفيين.

أهداف الدراسة:

استكشاف التحديات الأمنية التي تواجه غرف الأخبار في العصر الرقمي:

- تحديد أنواع الهجمات الإلكترونية الشائعة التي تستهدف غرف الأخبار.
- تحليل الثغرات الأمنية المحتملة في البنية التحتية التقنية والإجراءات المتبعة في غرف الأخبار.

استكشاف استراتيجيات وحلول لتعزيز الأمن السيبراني في غرف الأخبار:

- تحديد أفضل الممارسات والتدابير الأمنية التي يمكن تطبيقها في غرف الأخبار للتصدي للتهديدات الإلكترونية.
- اقتراح برامج تدريبية وتوعوية لرفع مستوى الوعي الأمني لدى الصحفيين وتعزيز مهاراتهم في هذا المجال.

الإجراءات المنهجية للدراسة:

تعتبر الدراسة دراسة وصفية تهدف إلى رصد وتفسير واقع الأمن السيبراني في غرف الأخبار .ويعتمد البحث على منهج المسح الإعلامي، لجمع البيانات من عينة من الصحفيين والعاملين في غرف الأخبار.

ولجمع البيانات تم تصميم أداة الاستقصاء وتطبيقها على الصحفيين والعاملين بالمؤسسات الإعلامية في مصر، حيث تم تطبيق الاستبيان إلكترونياً على عينة متاحة من الصحفيين والعاملين بغرف الأخبار بلغ عددها 225 مفردة، من المؤسسات الصحفية القومية والخاصة بمصر.

الإطار المعرفي للدراسة:

يتيح "الأمن السيبراني" لغرف الأخبار، من خلال إجراءات أمنية احترازية هامة، القدرة على التحكم بالمخاطر والتهديدات الإلكترونية إلى حد كبير، ومكافحة الجرائم الإلكترونية الناتجة عن استخدام تكنولوجيا الاتصال والمعلومات . فإهمال هذه الإجراءات قد يؤدي إلى نتائج كارثية، مثل الاختراق والقرصنة والابتزاز وسرقة البيانات والتعدي على الخصوصية والملكية الفكرية، وهي حوادث نسمع عنها بشكل يومي، وقد تستهدف أي فرد أو مؤسسة، بما في ذلك غرف الأخبار.

ومن خلال تعزيز الأمن السيبراني في غرف الأخبار، يمكن للمؤسسات الإعلامية ضمان سلامة عملياتها وبياناتها، وحماية صحفييها من التهديدات الإلكترونية، والحفاظ على مصداقيتها وسمعتها، وضمان استمراريتها في أداء رسالتها الإعلامية بكل حرية ومسؤولية في ظل التحديات المتزايدة في العصر الرقمي.

يعد مفهوم "الأمن الإلكتروني" أو الأمن السيبراني من المفاهيم الحديثة نسبياً والتي ظهرت في اطار الثورة الرقمية والتكنولوجية المعاصرة، والتي أدت إلى تدفق المعلومات بشكل كبير وغير مسبق، مع تعدد وسائل الاتصال الي مصادر المعلومات عبر أجهزة الحواسيب، وغيرها من الأجهزة المحمولة، وفي هذا السياق ظهر مفهوم الأمن السيبراني، ليعبر عن الجانب الأمني المرتبط بحماية تلك المعلومات، وحسب تعريف الهيئة الوطنية للأمن السيبراني يُعرف الأمن الإلكتروني بأنه (حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.) (المنتشري، 2020، ص102)

حيث أن كلمة سيبراني مشتقة من كلمة سايبر cyber والتي تعني إلكتروني وبإضافة أي كلمة لها تعطيها الصفة الإلكترونية، على سبيل المثال لا الحصر (cyber security) تعني الأمن الإلكتروني. (العبودي، 2019، ص92)

ولقد شاع استخدام مصطلح الأمن السيبراني كمرادف لأمن المعلومات، وذلك بعد أن انتشر مفهوم الفضاء السيبراني، الذي يرتبط ارتباطا وثيقا بالإنترنت وبتكنولوجيا الاتصالات والمعلومات. (العريشي، 2018، ص 303)

وهو مفهوم يتسع ليشمل حماية المعلومات من الضرر بكافة أشكاله، سواء كان مصدره أشخاصاً كالمحترفين، أو برامج كفيروسات الحاسب الآلي، وسواء كان متعمداً أم عن طريق الخطأ، وحماية المعلومات من الوصول لغير المصرح به، أو السرقة، أو التغيير أو إعادة التوجيه، أو سوء الاستخدام، وحماية قدرة المنشأة على الاستمرار وأداء أعمالها على أحسن وجه، وتمكين أنظمة تقنية المعلومات والبرامج التطبيقية لدى المنشأة من العمل بشكل آمن. (صالح، 2018، ص43)

ومن زاوية أكاديمية هو "ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تتهدد بها ومن أنشطة الاعتداء عليها، ومن زاوية تكنولوجيا هو "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية"، ومن زاوية قانونيه فإن الأمن الإلكتروني هي التدابير اللازمة لحماية سريه وسلامة المحتوى وتوفر المعلومات، ومكافحه أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض التشريعات لحماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها مثل جرائم الحاسوب والإنترنت. (لمين، 2009، ص165)

ومن المفاهيم السابقة يمكن القول أن مفهوم الأمن الإلكتروني يتكون من:

- الأمن الإلكتروني مفهوم يشمل أمن المعلومات، وأمن الشبكات، وأمن الأجهزة الإلكترونية.

- مجموعة من الاستراتيجيات تشمل إجراءات وقائية واحترازية تستخدم في المجال التقني.

- هي وسائل دفاعية لحماية المعلومات والبيانات والأجهزة الإلكترونية.

- يؤدى إلى صد ومكافحة الجرائم الإلكترونية بكافة أشكالها كـ (السرقة، والاختراق، والقرصنة، والاعتداء على المعلومات والأشخاص . . . إلخ)

- يهتم بحماية الأشخاص والمؤسسات من الهجمات الإلكترونية، وضمان أداء مهني جيد لهما، وذلك من خلال ضمان الاستخدام الآمن لتكنولوجيا المعلومات والاتصال.

♦ **أهمية الأمن الإلكتروني:**

1- توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.

2- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزه وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات.

3- توفير المتطلبات اللازمة للحد من الجرائم السيبرانية التي تستهدف المستخدمين.

4- مقاومه البرمجيات الخبيثة وما تستهدفه من أحداث أضرار بالغه بالمستخدمين وأنظمة المعلومات.

5- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومات والأفراد.

6- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها وسد الثغرات في أنظمة المعلومات. (صائغ، 2018، ص22)

7- حماية مصالح الدولة الحيوية والأمن الوطني والبني التحتية الحساسة فيها.

8- تعزيز حماية الشبكات وأنظمة المعلومات، وتعزيز حماية وسريته خصوصيه البيانات الشخصية.

9- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة. (الربيعة، 2017، ص13)

ومما تقدم يعتبر الأمن الإلكتروني ضرورة ملحة لكافة المؤسسات والأفراد، بل وأوسع من ذلك فهو من أسس البنى التحتية التكنولوجية للدولة، وتعد المؤسسة الصحفية والعاملين فيها جزء مؤثر بالمجتمع، لذلك ينبغي أن تحقق المؤسسة الصحفية كافة أهداف الأمن الإلكتروني للصحفيين العاملين بها، وذلك بهدف حماية الصحفيين من كافة أوجه الجرائم الإلكترونية، وأن تضمن لهم الاستخدام الآمن للأجهزة التكنولوجية وشبكة المعلومات، وتعزيز حماية خصوصية الصحفيين وبياناتهم الشخصية، كي لا تقع في الأيدي الخطأ ويتعرض الصحفي للابتزاز أو الانتحال أو التصيد الإلكتروني، وهنا نؤكد أن للأمن الإلكتروني أهمية قصوى لكافة الأفراد والمؤسسات وذلك بسبب التالي:

1- الحاجة إلى الارتباط بنظم الاتصالات والإنترنت وعدم إمكانية عزل الأجهزة عن الشبكات المحلية والشبكات واسعة النطاق لتوفير المعلومات لمن يحتاجها .

2- صعوبة تحدي الأخطار والتحكم بها أو متابعة المجرمين ومعاقبتهم؛ لعدم توافر الحدود الجغرافية حين استخدام الإنترنت والاتصالات الإلكترونية؛ لأنها تتيح الفرصة لاختراق الحدود الجغرافية.

3- النمو المطرد في الاستخدامات والتطبيقات الإلكترونية وظهور التجارة الإلكترونية والتسوق الشبكي والحكومة الإلكترونية والإدارة الإلكترونية التي تحتاج الي بيئة معلوماتية آمنة. (العوادي، 2016، ص7)

4- الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص العام.

5- النمو السريع في استخدام التطبيقات الإلكترونية والتي تتطلب بيئة آمنة - مع تطور التقنية المعلوماتية وازدهارها توفرت فرص الإجرام الإلكتروني. (العريشي، 2018، ص312)

الاحتياطات الأمنية اللازمة لتحقيق الأمن الإلكتروني ومكافحة الجرائم الإلكترونية على مستوى المؤسسات:

1- يجب تطبيق إجراءات أمنية مشددة من قبل الأفراد والمؤسسات لتحديد اهم المسائل التي يجب أن تتخذ لمواجهة الاختراقات.

2- الاستعانة بالمكاتب الاستشارية أو المؤسسات أو الشركات المعنية المتخصصة بأمن المعلومات والاتصالات لاتخاذ الإجراءات الأمنية الملائمة واللازمة لطبيعة عمل المؤسسة، بهدف دعم وسائل الحد من الاختراقات وحماية مراكز المعلومات بوسائل فعالة ومتطورة، وبذلك نضمن صعوبة الاختراق من قبل الأخرين. (العوادي، 2016، ص22)

3- يجب تأهيل كل المستخدمين وتوعيتهم وتدريبهم على استخدام نظم المعلومات التي تتمتع بمزايا الأمن والسرية؛ لما لذلك من أهمية في الحفاظ على أمن المعلومات وسريتها وحماية المستخدمين أنفسهم من الوقوع في المحظور دون قصد، وعلى المؤسسة وضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن الإلكتروني، بل أن المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الإجراءات المطلوبة من العاملين لدى ملاحظة أي خلل، كما أن عليها تحديد ما يتعين على المستخدمين القيام به وما يحظر عليهم القيام به في استخدام وسائل التقنية المختلفة (الدباغ، 2012، ص123)

4- توعية العاملين وتثقيفهم سواء أكانوا على مستوى أفراد أم مؤسسات بخطورة الاختراق وضرورة الحذر منه، ويجب تدريب العاملين في مراكز المعلومات الخاصة بالمؤسسات على كيفية اكتشاف الاختراقات وإيقافها، والحد من أخطارها والأضرار التي من الممكن أن تلحقها وأساليب التعرف على مرتكبيها، فضلا عن تدريبهم على الإجراءات الواجب اتباعها للحفاظ على المعلومات.

5- تحميل وتنصيب أحدث برامج الحماية الخاصة بأنظمة التشغيل لتدارك المشاكل والاختراقات، ويجب مراعاة تحديث هذه البرامج دوريا لغرض كشف الثغرات أو الفايروسات التي تساعد على عملية الاختراق. (العوادي، 2016، ص23)

6- التحكم في ملفات المشاركة المحلية بين الحاسبات ومحاولة إزالتها، لأنها أكبر مصدر للتهديد الأمني حيث تسمح لأي شخص بالدخول الي الجهاز الخاص بالمستخدم ومشاركة المعلومات الموجودة في ملفات المشاركة. (العوادي، 2016، ص23)

7- تتبع تطورات الجريمة الإلكترونية وتطوير الوسائل والتشريعات لمكافحتها. (خبازي، 2017، ص37) مما سبق نرى أن المؤسسات لها دور كبير في مواجهة الجرائم الإلكترونية والحد من تداعياتها ومخاطرها، فالمؤسسات الصحفية وما تمتلكه من مواقع إخبارية إلكترونية، وتعاملها الكبير بتكنولوجيا المعلومات الاتصال في كافة ممارساتها الصحفية اليومية، تجعلها أرض خصبة للتهديدات الإلكترونية، لذا يجب أن تضع المؤسسة الصحفية سياسة أمنية إلكترونية تحميها من مخاطر التهديدات الإلكترونية، وأيضا يمكن أن تسن تشريعات ضمن السياسة التحريرية للمؤسسة لضمان الأمن الإلكتروني بها، ويعتبر الاستعانة بالمستشارين التقنيين لمساعدتها في سد كافة الثغرات الأمنية بها، ومن جهة أخرى وضع دورات تدريبية أمر مهم لتدريب وتأهيل الصحفيين وكافة العاملين بالمؤسسة لمواجهة الجرائم الإلكترونية، وأيضا ينبغي للمؤسسات الصحفية تزويد أجهزة المؤسسة بأحدث نظم التشغيل الآمنة وبرامج الحماية وتحديثها باستمرار لسد الثغرات التي من خلالها تمكن المجرم من قرصنة واختراق الصحيفة وموقعها.

- **تحديات مكافحة الجرائم الإلكترونية:**

يلزم تطبيق مبادئ الأمن الإلكتروني عدة استراتيجيات واحتياطات أمنية ينبغي أن يطبقها الأفراد والمؤسسات لحماية أنفسهم من مخاطر وتهديدات الجرائم الإلكترونية، ولكن توجد عدة معوقات وتحديات تحول بين تطبيق

الأمن الإلكتروني، وهذه المعوقات تؤثر بالسلب على الاستخدام الآمن لتكنولوجيا الاتصال والمعلومات، ومن هذه المعوقات يمكن ذكرها كالتالي:

1- عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، وبالتالي عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم. (المطردي، 2012، ص21)

2- ظهور وتنامي الأنشطة الإجرامية الإلكترونية وتوسل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات.

3- تستعصي بعض هذه الأنشطة الإجرامية الإلكترونية على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

4- ظاهرة الجرائم الإلكترونية باتت تتخذ أنماطاً جديدة وضرباً من ضروب الذكاء الإجرامي وهذا بلا شك يمثل تحديا جدياً وجديداً في الوقت الحاضر.

5-هشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية (عطايا، 2015، ص375)

6- سهولة إخفاء الدليل وإعاقة الوصول إليه: حيث يمكن للمجرم المعلوماتي أن يجعل من الصعب الاحتفاظ بدليل الجريمة الإلكترونية، كما يمكنه في اقل من ثانية بل في لمحة من البصر أن يمسح أو يغير البيانات والمعلومات الموجودة في الكمبيوتر. (هشام، 2018، ص153)

7- خشية الجهات التي وقعت عليها الجرائم المعلوماتية، خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث في سمعتها ومصداقيتها وموقفها في السوق، وثقة السوق في قدرتها، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم.

8- خشية المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية.

9- بعض الضحايا قد تساوره الشكوك حول مقدرة رجال إنفاذ القانون على التعامل مع الجرائم المعلوماتية، بسبب اعتقادهم بعدم توفر الخبرة الفنية لدى رجل الضبط أو المحقق أو عدم توفر المعدات والتجهيزات اللازمة للتحقيق في هذا النوع من الجرائم.

10- الرغبة في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلا.

11- بعض الجرائم المعلوماتية ترتبط بجرائم أخلاقية، لذا يحجم المجني عليه من الإبلاغ اتقاء للفضيحة والعار. (الأطرش، 2018، ص638)

نتائج الدراسة:

أولاً: مناقشة وعي العاملين بغرف الأخبار بالمؤسسات الصحفية المصرية بأهمية الأمن السيبراني.

وعي العاملين بغرف الأخبار بأهمية الأمن السيبراني.	ك	%
لدي علم بتدابير وإجراءات الأمن الإلكتروني	96	%42.7
لدي معرفة بتشريعات وقوانين الجرائم الإلكترونية المصرية	132	%58.7
أهتم بمتابعة حالات اختراق تعرض لها بعض الصحفيين مؤخراً	145	%64.4
أعلم بوجود المجلس الأعلى للأمن السيبراني المصري لمكافحة الجرائم الإلكترونية	176	%78.2
اهتم بالتعرف على كل ما هو جديد في مجال الأمن الإلكتروني	95	%42.2
لا شيء مما سبق	21	%9.3

يوضح الجدول نتائج دراسة حول وعي العاملين في غرف الأخبار بأهمية الأمن السيبراني. و يمكن تحليل النتائج على النحو التالي: نسبة عالية (78.2%) من العاملين على دراية بوجود المجلس الأعلى للأمن السيبراني، مما يشير إلى وعي جيد بدور الجهات الرسمية في مكافحة الجرائم الإلكترونية. ويهتم غالبية العاملين (64.4%) بمتابعة حالات الاختراق التي يتعرض لها الصحفيون، مما يدل على إدراكهم للتهديدات الأمنية المحتملة. وأكثر من نصف العاملين (58.7%) لديهم معرفة بتشريعات وقوانين الجرائم الإلكترونية، و (42.7%) لديهم علم بتدابير وإجراءات الأمن الإلكتروني. نقاط الضعف: ويبدو أن الاهتمام بالتعرف على كل ما هو جديد في مجال الأمن السيبراني منخفض نسبياً (42.2%)، مما قد يعيق مواكبة التطورات في هذا المجال. وهناك نسبة (9.3%) لا تهتم بأي من الجوانب المتعلقة بالأمن السيبراني، مما يشكل تحدياً كبيراً. فبشكل عام تشير النتائج إلى وجود مستوى جيد من الوعي بأهمية الأمن السيبراني بين العاملين في غرف الأخبار، خاصة فيما يتعلق بالجوانب القانونية وحالات الاختراق. ومع ذلك، هناك حاجة لزيادة الاهتمام بالتعرف على كل ما هو جديد في مجال الأمن السيبراني، ورفع مستوى الوعي لدى الفئة غير المهتمة.

وتؤكد هذه النتائج على أهمية الاستثمار في برامج التوعية والتدريب على الأمن السيبراني للعاملين في غرف الأخبار .يجب أن تركز هذه البرامج على تزويد العاملين بالمعرفة والمهارات اللازمة للتعرف على التهديدات السيبرانية وتجنبها، بالإضافة إلى الإبلاغ عن أي حوادث أمنية محتملة .كما يجب أن تشجع هذه البرامج على تبني ثقافة أمنية إيجابية في غرف الأخبار، حيث يدرك كل فرد دوره في حماية أمن المعلومات.

من المهم أيضًا أن تتعاون المؤسسات الإعلامية مع الجهات المعنية بالأمن السيبراني، مثل المجلس الأعلى للأمن السيبراني، لتبادل المعلومات والخبرات وأفضل الممارسات في هذا المجال .يمكن أن يساهم هذا التعاون في تعزيز الأمن السيبراني لوسائل الإعلام وحماية حرية التعبير

ثانياً: مناقشة التحديات السيبرانية التي تواجه العاملين بغرف الأخبار بالمؤسسات الصحفية المصرية.

التحديات السيبرانية التي تواجه العاملين بغرف الأخبار.	ك	%
انتهاك خصوصية الصحفيين وتعرضهم للسب والتشهير	188	%83.6
التجسس والتنصت ومراقبة المكالمات الهاتفية وسرقة المحادثات الإلكترونية	167	%74.2
انتحال شخصية الصحفيين على مواقع التواصل الاجتماعي	164	%72.9
التصيد والخداع للحصول على معلومات وبيانات وصور شخصية	145	%64.4
الابتزاز الإلكتروني والتهديد والتخويف بنشر الفضائح أو الصور أو المحادثات	152	%67.6
سرقة الموضوعات والتحقيقات الصحفية ونشرها على مواقع أخرى	220	%97.8
التلاعب بالمحتوى والمعلومات والأرقام والصور المضللة	138	%61.3
نشر الفيروسات وتدمير البيانات على الأجهزة	103	%45.7
اختراق المواقع الإخبارية لنشر الشائعات والأخبار الزائفة للتخويف وزعزعة الاستقرار والأمن	207	%92
جرائم الاحتيال الإلكتروني وسرقة الأموال	111	%49.3
قرصنة الموقع الصحفي وتعطيله عن العمل	198	%88
اختراق حسابات الصحفيين على مواقع التواصل الاجتماعي والبريد الإلكتروني	204	%90.7
مراقبة التنقل والموقع الجغرافي GPS	35	%15.5

من هذا الجدول يتصدر قائمة التحديات "سرقة الموضوعات والتحقيقات الصحفية ونشرها على مواقع أخرى" بنسبة مقلقة بلغت 97%.8، مما يشير إلى تعرض الصحفيين لسرقة جهودهم وأعمالهم بشكل كبير .يتبع ذلك "اختراق المواقع الإخبارية لنشر الشائعات والأخبار الزائفة للتخويف وزعزعة الاستقرار والأمن" بنسبة 92%، مما يؤكد استخدام الفضاء الإلكتروني كسلاح لنشر المعلومات المضللة وتهديد الأمن .كما يبرز "اختراق حسابات الصحفيين على مواقع التواصل الاجتماعي والبريد الإلكتروني" بنسبة 90 7%.و"انتهاك خصوصية

الصحفيين وتعرضهم للسب والتشهير" بنسبة 83 6%.كتهديدات خطيرة تستهدف الصحفيين بشكل شخصي ومهني.

تتضمن التحديات الأخرى ذات النسب المرتفعة "التجسس والتنصت ومراقبة المكالمات الهاتفية وسرقة المحادثات الإلكترونية" و"انتحال شخصية الصحفيين على مواقع التواصل الاجتماعي" و"التصيد والخداع للحصول على معلومات وبيانات وصور شخصية" و"الابتزاز الإلكتروني والتهديد والتخويف بنشر الفضائح أو الصور أو المحادثات"، مما يشير إلى تنوع أساليب الهجمات السيبرانية التي يتعرض لها الصحفيون.

على الجانب الآخر، تأتي "نشر الفيروسات وتدمير البيانات على الأجهزة" و"التلاعب بالمحتوى والمعلومات والأرقام والصور المضللة" و"جرائم الاحتيال الإلكتروني وسرقة الأموال" و"قرصنة الموقع الصحفي وتعطيله عن العمل" بنسب أقل، إلا أنها لا تزال تشكل تهديدات يجب أخذها على محمل الجد .وأخيرًا، يعتبر "مراقبة التنقل والموقع الجغرافي "GPS التحدي الأقل شيوعًا بنسبة 15%5.، لكنه يثير مخاوف بشأن انتهاك الخصوصية وتتبع الصحفيين.

وتسلط هذه النتائج الضوء على مشهد مقلق يواجه العاملين في غرف الأخبار، حيث تتجلى التحديات السيبرانية كتهديد متزايد لسلامتهم الشخصية والمهنية، وعرقلة لحرية الصحافة. ونذكرها كالتالي:

سرقة المحتوى والتحقيقات الصحفية :تشير هذه الظاهرة إلى استهداف مباشر لجهود الصحفيين ومصداقيتهم، مما قد يثنيهم عن القيام بعملهم الاستقصائي ويحد من قدرتهم على كشف الحقائق.

نشر الشائعات والأخبار الزائفة :يوضح هذا التحدي كيف يمكن استخدام الفضاء الإلكتروني كأداة للتضليل والتلاعب بالرأي العام، مما يضعف الثقة في وسائل الإعلام ويهدد استقرار المجتمعات.

اختراق الحسابات وانتهاك الخصوصية :يمثل هذا التحدي انتهاكًا صارخًا لخصوصية الصحفيين وحرياتهم الشخصية، مما يعرضهم للخطر ويقوض قدرتهم على العمل بحرية.

التجسس والتنصت والابتزاز الإلكتروني :تشير هذه التحديات إلى استخدام أساليب متطورة للتجسس على الصحفيين وتهديدهم وابتزازهم، مما يخلق بيئة عمل عدائية وغير آمنة.

التلاعب بالمحتوى والمعلومات :يمثل هذا التحدي تهديدًا لمصداقية العمل الصحفي، حيث يمكن التلاعب بالمعلومات والصور لتشويه الحقائق وتضليل الجمهور.

الفيروسات والاحتيال الإلكتروني وقرصنة المواقع :تشكل هذه التحديات تهديدات تقنية مباشرة لعمل غرف الأخبار، حيث يمكن أن تؤدي إلى تعطيل العمل وتدمير البيانات وسرقة الأموال.

مراقبة التنقل والموقع الجغرافي :يثير هذا التحدي مخاوف بشأن تتبع الصحفيين ومراقبة تحركاتهم، مما يحد من قدرتهم على العمل بحرية واستقصاء المعلومات الحساسة.

ثالثاً: مناقشة استراتيجيات العاملين بغرف الأخبار تجاه الأمن السيبراني.

استراتيجيات العاملين بغرف الأخبار تجاه الأمن السيبراني	ك	%
أبلغ الجهات المختصة كالمؤسسة أو النقابة	144	%64
أبلغ الجاهات والأجهزة الأمنية	143	%63.6
أتوجه لخبير تكنولوجي فوراً	121	%53.8
أطلب المساعدة من الأصدقاء	95	%42.2
أغلق الحسابات لفترة مؤقتة	60	%26.7
أغير كلمة المرور بسرعة	128	%56.9
لا استخدم الجهاز لحين تأمينه وإصلاحه	62	%27.6
أبحث على الإنترنت لحل لهذه المشكلة	83	%36.9
لا أهتم	19	%8.4

يوضح الجدول استراتيجيات العاملين بغرف الأخبار تجاه الأمن السيبراني، و يمكن تحليل هذه النتائج كما يلي:

الإبلاغ والبحث عن مساعدة فنية: يظهر الجدول أن رد الفعل الأكثر شيوعًا للصحفيين عند التعرض لجريمة إلكترونية هو إبلاغ الجهات المختصة سواء كانت المؤسسة التي يعملون بها أو النقابة (66.4%) أو الجهات والأجهزة الأمنية (63.6%)، يلي ذلك التوجه لخبير تكنولوجي (53.8%). وهذا يشير إلى وعي بأهمية الإبلاغ عن هذه الجرائم والبحث عن مساعدة فنية متخصصة للتعامل معها.

الإجراءات الوقائية: يتخذ الصحفيون أيضًا إجراءات وقائية فورية، حيث يقومون بتغيير كلمة المرور بسرعة (56.9%) وإغلاق الحسابات لفترة مؤقتة (26.7%) وعدم استخدام الجهاز حتى يتم تأمينه وإصلاحه (27.6%). وهذا يدل على وعي بأهمية اتخاذ خطوات سريعة للحد من الضرر المحتمل.

الاعتماد على الذات والإنترنت: يلجأ بعض الصحفيين إلى البحث على الإنترنت لحل المشكلة بأنفسهم (36.9%) أو طلب المساعدة من الأصدقاء (42.2%). وهذا قد يكون مفيدًا في بعض الحالات البسيطة، ولكنه قد لا يكون كافيًا في حالات الجرائم الإلكترونية الأكثر تعقيدًا.

عدم الاكتراث: هناك نسبة ضئيلة (8.4%) من الصحفيين لا تهتم عند التعرض لجريمة إلكترونية. وهذا يشير إلى عدم إدراك خطورة هذه الجرائم والعواقب المحتملة لها على الصحفيين وعملهم.

النتائج العامة :

انطلاقًا مما سبق، يُشدد الباحث على أن توافر الأمن السيبراني بغرف الأخبار الصحفية في مصر يُقدم مميزات عديدة للمؤسسة، تنعكس إيجابًا على المشهد الإعلامي ككل:

1. حماية المعلومات الحساسة :

تتعامل غرف الأخبار الصحفية في مصر مع كم هائل من المعلومات الحساسة، بما في ذلك البيانات الشخصية للمصادر، والمعلومات السرية المُتعلقة بالتحقيقات الصحفية، خاصة تلك التي تتناول قضايا الفساد أو الأمن القومي. ويضمن الأمن السيبراني القوي حماية هذه المعلومات من السرقة، أو التسريب، أو التلاعب بها من قبل جهات داخلية أو خارجية. ويُعد هذا الأمر بالغ الأهمية في مصر للحفاظ على مصداقية المؤسسات الإعلامية، وحماية سلامة المصادر التي تُخاطر بالكشف عن معلومات هامة، لاسيما في ظل التحديات التي تواجه حرية الصحافة.

2. الحفاظ على استمرارية العمل :

تعتمد غرف الأخبار في مصر بشكل مُتزايد على التكنولوجيا والبنية التحتية الرقمية لإنتاج ونشر الأخبار، خاصةً مع انتشار منصات التواصل الاجتماعي. يُمكن أن تُؤدي الهجمات السيبرانية، مثل هجمات حجب الخدمة، إلى تعطيل هذه الأنظمة، مما يُؤثر سلبًا على قدرة المؤسسة على أداء عملها وتقديم الأخبار للجمهور المصري في الوقت المناسب. ويضمن الأمن السيبراني القوي استمرارية العمل وعدم انقطاع تدفق المعلومات، وهو أمر ضروري في ظل الأحداث المُتسارعة التي تشهدها مصر والمنطقة.

3. مكافحة التضليل الإعلامي :

تُواجه غرف الأخبار في مصر تحديًا كبيرًا في مكافحة التضليل الإعلامي، خاصةً على منصات التواصل الاجتماعي. وغالبًا ما تكون هذه المؤسسات هدفًا لحملات مُمنهجة تهدف إلى نشر أخبار كاذبة أو مُضللة، أو تشويه سمعة المؤسسة والعاملين بها. ويُساعد الأمن السيبراني القوي على اكتشاف ومُنع هذه الهجمات، من خلال رصد الحسابات الوهمية والصفحات المُزيفة، وتحليل المحتوى المُضلل، مما يُحافظ على مصداقية المؤسسة الإعلامية ويُساهم في مكافحة انتشار المعلومات المُضللة التي تُؤثر على الرأي العام في مصر.

4. حماية حرية الصحافة :

يتعرض الصحفيون في مصر للمُراقبة والتجسس والهجمات الإلكترونية بسبب طبيعة عملهم، خاصةً عند تناولهم لقضايا حساسة. ويُساعد الأمن السيبراني القوي على حماية الصحفيين ومصادرهم من خلال تأمين الاتصالات، وتشفير البيانات، واستخدام أدوات تُخفي الهوية على الإنترنت. ويُمكن هذا الدعم الصحفيين من أداء عملهم بحرية ودون خوف من المُلاحقة أو التضييق، مما يُعزز دور الصحافة كسلطة رابعة تُساهم في مُراقبة أداء الحكومة والمؤسسات، وتُعزز الشفافية والمُساءلة في مصر.

وبالرغم من مميزات الأمن السيبراني لغرف الأخبار، إلا أنه يواجه عدة تحديات نذكر منها:

يأتي نقص الوعي والموارد كأحد أهم التحديات، حيث لا يزال الوعي بأهمية الأمن السيبراني محدودًا لدى بعض الصحفيين والعاملين في غرف الأخبار، خاصةً في المؤسسات الصحفية الصغيرة والمتوسطة. ويُضاف إلى ذلك محدودية الميزانيات المُخصصة للأمن السيبراني، إذ تُعاني العديد من المؤسسات الصحفية المصرية من نقص التمويل، مما ينعكس سلبًا على قدرتها على شراء البرامج والأدوات اللازمة، وتوظيف خبراء مُتخصصين في هذا المجال.

وعلى الصعيد التقني، نرى أن الاعتماد على البرامج المُقرصنة، بسبب ارتفاع تكلفة البرامج الأصلية، يُعرّض المؤسسات الصحفية لخطر الإصابة بالبرمجيات الخبيثة والاختراقات الأمنية. وتُواجه بعض غرف الأخبار أيضًا صعوبة في تأمين الأجهزة القديمة التي لا تزال قيد الاستخدام، مما يجعلها أكثر عُرضة للاختراقات الأمنية.

وفيما يتعلق بالإطار القانوني والتنظيمي، فعلى الرغم من إصدار قوانين مكافحة جرائم تقنية المعلومات، إلا أن التشريعات المُتعلقة بالأمن السيبراني في مصر لا تزال حديثة العهد، وتُواجه الجهات المعنية أيضًا تحدياتٍ في تطبيق القوانين على أرض الواقع، خاصةً في ظل صعوبة تتبع مُرتكبي الجرائم الإلكترونية وتحديد هويتهم.

ويبرز تحدٍ آخر يتمثل في ضرورة إيجاد توازنٍ دقيق بين مُتطلبات الأمن القومي وحماية البيانات من جهة، وحرية الصحافة وحق الوصول إلى المعلومات من جهة أخرى عند وضع وتنفيذ سياسات الأمن السيبراني.

كما أن انتشار الشائعات والمعلومات المُضللة يُشكل بيئةً خصبةً تزيد من صعوبة مهمة غرف الأخبار في التحقق من المعلومات ومكافحة التضليل الإعلامي. ولا يُمكن هنا إغفال تعرض غرف الأخبار في مصر لهجماتٍ إلكترونية مُنظمة ومدعومة من جهاتٍ تهدف إلى زعزعة الاستقرار أو التأثير على الرأي العام. والمؤسسات الصحفية والمجتمع المدني والمنظمات الدولية.

استراتيجيات لتعزيز الأمن السيبراني في غرف الأخبار:

أولًا: استراتيجية التدريب والتوعية المستدامة:

تُعد هذه الاستراتيجية حجر الأساس في بناء ثقافة أمنية قوية داخل غرف الأخبار. لا يقتصر الأمر على مجرد تنظيم برامج تدريبية فحسب، بل يتعداه إلى خلق منظومة متكاملة تضمن استدامة الوعي الأمني. ويشمل ذلك تنظيم برامج تدريبية دورية وشاملة لجميع العاملين، من صحفيين ومحررين وفنيين وإداريين. ويجب أن تُغطي هذه البرامج مختلف جوانب الأمن السيبراني، بدءًا من التعريف بالتهديدات السيبرانية المُحتملة، مرورًا بأساليب الوقاية منها، ووصولًا إلى أفضل الممارسات الأمنية في العمل اليومي. كما ينبغي أن تتضمن البرامج تدريبات عملية على كيفية التعامل مع الهجمات في حال وقوعها، وكيفية الإبلاغ عنها بشكل سليم. إلى جانب البرامج التدريبية، ويجب نشر الوعي بشكل مستمر من خلال حملات توعية داخلية، تتضمن رسائل بريد إلكتروني تذكيرية، وملصقات توعوية تُوزع في أماكن العمل، بالإضافة إلى نشرات دورية تتناول أحدث التطورات في

مجال الأمن السيبراني وأفضل الممارسات للتعامل معها. ويجب أن تُصمم هذه الحملات بأسلوب سهل وجذاب يُشجع على التفاعل والمشاركة.

ثانيًا: استراتيجية التحصين التقني وتحديث الأنظمة:

تُمثل هذه الاستراتيجية الدرع التقني الذي يحمي البنية التحتية لغرف الأخبار من الهجمات السيبرانية. وتبدأ هذه الاستراتيجية بضمان تحديث جميع البرامج وأنظمة التشغيل بشكل دوري ودائم، بما في ذلك أنظمة إدارة المحتوى، وبرامج تحرير النصوص والصور، وأنظمة البريد الإلكتروني. يُعد هذا التحديث ضروريًا لسد الثغرات الأمنية المعروفة التي قد يستغلها المُخترقون. كما تشمل تثبيت وتحديث برامج مكافحة الفيروسات وجدران الحماية على جميع أجهزة الحاسوب والخوادم، مع التأكد من تفعيل خاصية الفحص التلقائي للملفات والبرامج. ولمزيد من الحماية، ويجب استخدام كلمات مرور قوية وفريدة لكل حساب، تتكون من مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز، مع تغييرها بشكل دوري. ويُعد تشفير البيانات الحساسة، مثل المعلومات الشخصية للصحفيين ومصادرهم، أمرًا بالغ الأهمية، سواء أثناء تخزينها على الأجهزة أو أثناء إرسالها عبر الشبكة. ولضمان عدم فقدان البيانات في حال وقوع هجوم أو حدوث عطل تقني، ويجب إجراء نسخ احتياطي مُنتظم للبيانات الهامة، وتخزينها في مكان آمن، سواء على خوادم محلية أو على منصات تخزين سحابية موثوقة.

ثالثًا: استراتيجية السياسات والإجراءات الأمنية المُحكمة:

تُمثل هذه الاستراتيجية الإطار التنظيمي الذي يضمن تطبيق معايير الأمن السيبراني داخل غرف الأخبار. تبدأ بوضع سياسات أمنية واضحة وشاملة تُحدد مسؤوليات كل فرد، وتُوضح الإجراءات المُتبعة في مختلف المواقف. يجب أن تشمل هذه السياسات قواعد استخدام الإنترنت والبريد الإلكتروني، وإجراءات التعامل مع البيانات الحساسة، وسياسات إدارة كلمات المرور، وخطط الاستجابة للحوادث الأمنية. ولضمان فعالية هذه السياسات، ويجب إجراء تقييم دوري للمخاطر الأمنية، وتحديث السياسات والإجراءات بناءً على نتائج التقييم. كما يُعد تطبيق مبدأ "أقل امتيازات ممكنة" ضروريًا، حيث يتم منح كل مُستخدم الصلاحيات اللازمة لأداء عمله فقط، مما يُقلل من الأضرار المُحتملة في حال اختراق أحد الحسابات. وأخيرًا، يجب وضع خطة مُفصلة للتعامل مع الحوادث الأمنية، وتدريب جميع العاملين على كيفية تطبيقها بشكل فعال، بما في ذلك خطوات الإبلاغ عن الحادث، وعزل الأنظمة المُتضررة، واستعادة البيانات من النسخ الاحتياطية.

رابعًا: استراتيجية التعاون وتعزيز ثقافة المسؤولية المشتركة:

تعتمد هذه الاستراتيجية على مبدأ أن الأمن السيبراني مسؤولية الجميع وليست حكرًا على قسم تكنولوجيا المعلومات. ولتحقيق ذلك، ويجب بناء علاقات تعاون قوية مع الجهات الأمنية المُختصة، مثل المجلس الأعلى للأمن السيبراني، لتبادل المعلومات والاستفادة من خبراتهم وتوجيهاتهم في مجال الأمن السيبراني. كما يُنصح بالمشاركة الفعالة في المبادرات والفعاليات التي تهدف إلى تعزيز الأمن السيبراني في قطاع الإعلام بشكل عام. ولترسيخ ثقافة المسؤولية المُشتركة، يجب خلق بيئة عمل إيجابية تُشجع جميع العاملين على الإبلاغ عن أي

حوادث أمنية مُحتملة، أو ثغرات أمنية مُكتشفة، دون خوف من العقاب أو المُساءلة. وأخيرًا، يجب التأكيد بشكل مستمر على أن الأمن السيبراني هو مسؤولية كل فرد في غرفة الأخبار، وأن الالتزام بالسياسات والإجراءات الأمنية هو واجب على الجميع دون استثناء.

المراجع:

1. أحمد، وسام محمد.(2020).إدراك الصحفيين للمخاطر الرقمية وإستراتيجيات تطبيقهم للأمن الرقمي في عملهم المهني.**المجلة العربية لبحوث الإعلام والاتصال**، العدد 31، أكتوبر/ديسمبر، ص450:ص547
2. الأزرق، نرمين نبيل.(2020).التهديدات الرقمية ضد الصحفيين المصريين ووعيهم بالآليات المستخدمة للحفاظ على سلامتهم-دراسة كيفية.**مجلة البحوث الإعلامية**، جامعة الأزهر، العدد 54، الجزء 6،يوليو،ص4299:ص4338.
3. الاطرش، عصام حسني.(2018).معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية. **مجلة جامعة الشارقة للعلوم القانونية**، جامعة الشارقة، العدد 1، المجلد 16، يونيو 2019، ص632: 662.
4. خبازي، فاطمة الزهرة.(2017).جرائم الدفع الإلكتروني وسبل مكافحتها.**أعمال الملتقي الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري**، مركز جيل البحث العلمي، الجزائر، 29 مارس.
5. الدباغ، رائد عبدالقادر حامد. وبشرى علي زينل.(٢٠١٢).فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات. **مجلة تنمية الرافدين**، جامعة الموصل، كلية الإدارة والاقتصاد، مجلد ٣٤ ،العدد١١، ص123-140
6. الربيعة، صالح بن علي.(2017).الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت.الرياض: هيئة الاتصالات وتقنية المعلومات.
7. صالح، أحمد حسني.(2018).أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعات الأردنية.**رسالة ماجستير غير منشورة**،كلية العلوم التجارية،جامعة السودان للعلوم والتكنولوجيا.
8. صائغ، وفاء بنت حسن.(٢٠١٨). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية.**المجلة العربية للعلوم الاجتماعية**،المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية،المجلد٣، العدد ١٤، يوليو، ص، ٧٠:١٨.
9. العبودي، علي عبدالرحيم.(2019).هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين. **مجلة قضايا سياسية**، جامعة بغداد، كلية العلوم السياسية، العدد 57، ص374-345 .
10. العريشي، جبريل حسن.(2018).دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع.**مجلة الملك فهد الوطنية**، المجلد 24، العدد 2، سبتمبر، ص 302 – 373.
11. العريشي، جبريل حسن.(2018).دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع.**مجلة الملك فهد الوطنية**، المجلد 24، العدد 2، سبتمبر، ص 302 – 373.
12. عطايا، إبراهيم رمضان إبراهيم.(2015).الجريمة الإلكترونية - سبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية. **مجلة كلية الشريعة والقانون بطنطا**، جامعة الأزهر، العدد 30، الجزء 2، ص403،360.
13. العوادي، أوس نجيب غالب.(2016).الأمن المعلوماتي السيبراني.بغداد:سلسلة إصدارات مركز البيان للدراسات والتخطيط.
14. العوادي، أوس نجيب غالب.(2016).الأمن المعلوماتي السيبراني.بغداد:سلسلة إصدارات مركز البيان للدراسات والتخطيط.
15. لمين، عوطي.(2009). تحديات الأمن الإلكتروني في المؤسسة. **مجلة أبحاث اقتصادية وإدارية**، جامعة محمد خضير بسكرة، كلية العلوم الاقتصادية والتجارية وعلوم التيسير ، العدد 6،ديسمبر،ص 160-178.

16. المطردي، مفتاح ابوبكر.(2012).الجريمة الإلكترونية والتغلب على تحدياتها.**المؤتمر الثالث لرؤساء المحاكم العليا في الدولة العربية بجمهورية السودان**، من 23 الي 25 -9-2012.

17. المنتشري، فاطمة يوسف.(٢٠٢٠).درجه وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينه جده من وجهه نظر المعلمات.**المجلة العربية للتربية النوعية**،المجلد٤، العدد١٤، يوليو،ص ٩٥: ١٤٠.

18. المنتشري، فاطمة يوسف.(2020).دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. **المجلة العربية للعلوم التربوية والنفسية**، السعودية، المجلد 4، العدد 17، يوليو، ص. 457-484.

19. هشام، فريجة محمد.(2018).النظـــام القانونـــي للجريمـــة المعلوماتيـــة وصعوبات تحقيق الأمن الإلكتروني. **حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية**، الجزائر، جامعة المسيلة، العدد 24،ص 141-163.

20. Caine, K .McGregor, S. E., Roesner, F., &. (2016). Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proc. Priv. Enhancing Technol.*, *2016*(4), p418-435.

21. Chen, Y. (2020). Sounding the Alarm for "Watchdogs": Threats to Journalists' Digital Safety and Protection Strategies (Doctoral dissertation, Georgetown University).

22. Christofoletti, R., & Torres, R. J. (2018). Journalists exposed and vulnerable: digital attacks as a form of professional risk/Jornalistas expostos e vulneraveis: ataques digitais como modalidade de risco profissional. *Revista Famecos-Midia, Cultura e Tecnologia*, *25*(3), NA-NA.

23. Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., & Deibert, R. (2020). The information security cultures of journalism. *Digital Journalism*, *8*(8), p1068-1091.

24. INTERNEWS CENTER FOR INNOVATION & LEARNING. (2012). Digital security & journalists: a snapshot of awareness & practice in Pakistan. Retrieved from https://www.internews.org/sites/default/files/resources/Internews_PK_Secure_Journalist_2012-08.pdf

25. Lundberg, E., & Sadikovic, A. (2017). Vem skyddar vi källan från? : En kvalitativ studie om digital säkerhet och källskydd bland svenska journalister (Dissertation). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-p32885

26. McGregor, S. E., Watkins, E. A., & Caine, K. (2017). Would You Slack That? The Impact of Security and Privacy on Cooperative Newsroom Work. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW),p 1-22.

27. MILOSAVLJEVIĆ, M., Prodnik, J. A., & Kučić, L. J. (2015). SECURING THE COMMUNICATION OF JOURNALISTS WITH THEIR SOURCES AS A FORM OF SOURCE PROTECTION–EDITORIAL POLICY OF SLOVENIAN MEDIA REGARDING COMMUNICATION AND TECHNOLOGY. *Teorija in Praksa*, *52*(4), p612-30.

28. Mitchell McGregor, S. E., Watkins, E. A., & Caine, K. (2017). Would You Slack That? The Impact of Security and Privacy on Cooperative Newsroom Work. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW),p 1-22.

29. Roesner, F. & McGregor, S. T. H., Charters, P. (2015). Investigating the security needs and practices of journalists. This paper is included in the Proceedings of the 24th USENIX Security Symposium August 12–14, 2015 • Washington, D.C.

30. Shere, A. R., Nurse, J. R., & Flechais, I. (2020). " Security should be there by default": Investigating how journalists perceive and respond to risks from the Internet of Things. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 240-249). IEEE.

31. Waters, S. (2018). The effects of mass surveillance on journalists' relations with confidential sources: a constant comparative study. Digital Journalism, 6(10),p 1294-1313.

عن الدورية

- النشر الدوري: تصدر المجلة المصرية لبحوث الاتصال والإعلام الرقمي بصفة دورية (ثلاث مرات سنوياً)، وتنشر أبحاثًا باللغتين العربية والإنجليزية، مما يضمن استمرارية النشر وتوفير أحدث الأبحاث والدراسات للقراء والباحثين من مختلف أنحاء العالم.
- تنوع المحتوى: تقبل المجلة سبع تخصصات للنشر فيها وهي:

1. الإذاعة الرقمية
2. الإعلام
3. التسويق الرقمي
4. العلاقات العامة الرقمية
5. الصحافة الرقمية
6. تلفزيون الإنترنت
7. راديو الإنترنت

- النشر الإلكتروني والمفتوح: تُتاح المجلة المصرية لبحوث الاتصال والإعلام الرقمي للنشر الإلكتروني بنظام الوصول المفتوح (open access online) ، مما يضمن سهولة الوصول إليها وقراءتها وتحميلها مجانًا من قبل الباحثين والمهتمين في جميع أنحاء العالم.
- التنوع في أنواع المقالات: تنشر المجلة مجموعة متنوعة من أنواع المقالات، بما في ذلك:
- الأبحاث الأصلية (Original Articles): وهي أبحاث تقدم نتائج جديدة ومبتكرة في مجال الاتصال والإعلام الرقمي.
- المقالات المرجعية (Review Articles): وهي مقالات تستعرض وتلخص وتحلل مجموعة من الأبحاث السابقة حول موضوع معين.
- تقارير الحالة (Case Studies): وهي دراسات معمقة لحالات فردية أو أحداث معينة في مجال الاتصال والإعلام الرقمي.
- المقابلات مع خبراء وباحثين بارزين: في مجال الاتصال والإعلام الرقمي، لتقديم رؤيتهم حول أحدث التطورات والاتجاهات في هذا المجال.
- الأعداد الخاصة: تصدر المجلة أعدادًا خاصة حول موضوعات معينة ذات أهمية خاصة في مجال الاتصال والإعلام الرقمي، وذلك لجذب انتباه الباحثين والمهتمين إلى هذه الموضوعات وتشجيع البحث فيها.

بيانات الاتصال:

الموقع الإلكتروني: https://ejrcds.journals.ekb.eg

البريد الإلكتروني لهيئة التحرير: fatmaelzahrasaleh@art.sohag.edu.eg

البريد الإلكتروني للقسم: media.dep@art.sohag.edu.eg

العنوان: جامعة سوهاج، كلية الآداب، قسم الإعلام، مصر.