واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني

مداخل زيد عبد الرحيم التيماني

جامعة الملك سعود

الرياض–المملكة العربية السعودية

ملخص البحث

استهدف هذا البحث معرفة واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات ، وترجع أهمية هذا البحث ل تفاقم المهددات وكثرة الاختراقات وتواترها على كل الأصعدة وعلى كافة المستويات من الفرد إلى المؤسسات والوزارات والشركات- فقد بدأت الحكومات والشركات تعي تدريجياً أخطار الجرائم السيبرانية، وأهمية الأمن المعلوماتي على الأمن الاقتصادي والسياسي للبلد، وعلى المصالح العامة فقد يبدو الإنترنت جنة لمخترقي الشبكات؛ بسبب ظهورهم عليها ظهورًا فتراضيا، مغفلاً دون اسم، وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السيبرانية، وتدني أخطار ونسب اكتشافها، وصعوبة إثباتها في بعض الدول، لما تتسم به الجرائم السيبرانية من السرعة التي تتم بها، إذ قد تحدث الأضرار حتى قبل أن تعي الضحية استهدافها.

وقد استخدمت الباحثة في هذه الدراسة المنهج الوصفي ، وأداة المقابلة المطبقة على عينة من الخبراء المختصين بالأمن السيبراني في مدينة الرياض ، وقد كانت أهم النتائج التي توصلت إليها هذه الدراسة أن الاهتمام الحكومي بموضوع الأمن السيبراني بدأ بشكل مبكر قبل أن يدرك الافراد في المجتمع هذا المفهوم ، وأن أكثر أنماط الجرائم السيبرانية انتشارا بين الأفراد في المجتمع السعودي هي جريمة الاحتيال الإلكتروني ، كما توصلت الدراسة إلى أن أكثر العوامل التي تزيد من فرصة حدوث الجرائم السيبرانية هو ضعف الوعي لدى الأفراد ومشاركتهم المعلومات الشخصية مع الآخرين دون دراية ومعرفة بطبيعة عمل هؤلاء الأشخاص.

الكلمات المفتاحية: الوعي المعلوماتي، الأمن المعلوماتي، الأمن السيبراني، الجرائم السيبرانية.

المقدمة

شهدت المجتمعات الإنسانية خلال فترة تطورها نمواً ملحوظاً في جميع جوانب الحياة الاجتماعية ، مما ساعد على انتقالها من مجتمعات تقليدية تسودها حالة من البساطة في تعاملاتها وعلاقاتها بالبيئة الطبيعية وبالأفراد ،إلى مجتمعات صناعية تسودها حالة من التعقيد وتقسيم العمل والتي أنتجت لنا شكلاً آخر من أشكال التفاعل الإنساني والاجتماعي، فقد كان الأفراد يتفاعلون مع بعضهم البعض بشكل مباشر وجهاً لوجه ويقومون بإنهاء جميع تعاملاتهم وعلاقاتهم على هذا الأساس من التفاعل المباشر واستمر هذا الشكل حتى نمت المجتمعات وتطورت وارتقتوانعكس ذلك على البناء الاجتماعي وما يتصل بهذا البناء من عمليات اجتماعية، فأنتجت لنا بطبيعة الحال شكلاً مغايراً للتفاعل الاجتماعي الذي كان يعرفه البشر في المجتمعات التقليدية، فاتسم هذا التفاعل بالتركيب والتعقيد؛ وذلك نظراً لما أنتجته المجتمعات الصناعية من مخترعات واكتشافات أدت إلى إحداث التغير في التفاعل الاجتماعي بين الأفراد.

وحسب العالم دوركايم(الحسن، 2015) صاحب نظرية :(تقسيم العمل في المجتمع) نجد أن المجتمعات عندما تحولت من مرحلة إلى أخرى،أي من مجتمعات ميكانيكية ضيقة النطاق إلى مجتمعات عضوية واسعة النطاق نتج عن هذا التحول مجموعة من التغيرات الجذرية التي طالت النظم والعلاقات ، وأنتجت مؤسسات جديدة وافدة على المجتمع لم يعرفها البشر من قبل ، كالمؤسسات التعليمية والصحية والخدمية والمالية والعسكرية المتخصصة في تسهيل التعاملات بين الأفراد وبين الأفراد والحكومات.

هذه المؤسسات الحديثة والمرتبطة بالمجتمعات الصناعية لعبت دوراً مهماً في الأنماط السلوكية للأفراد والأدوار الاجتماعية التي يقومون بها، حيث أتاحت الثورة التقنية والتكنولوجية تغيير الحياة الاجتماعية بما تضم من نظم وعلاقات و أدوار، سمحت للأفراد الأخذ بسمات هذا المجتمع الحديث ؛ فاستفادوا من العلم الحديث وطورا العديد من الأنشطة الاقتصادية والصناعية ، وازداد الإنتاج ونمت قطاعات حيوية بالمجتمعات حتى أصبحت هي المسيطرة على حياة الأفراد في جميع تعاملاتهم.

وبالنظر إلى واقع التقنية الحديثة ، وفي ظل ثورة الاتصالات والمعلومات والتي جعلت من العالم قرية كونية واحدة أصبح جميع سكان الأرض يتفاعلون مع بعضهم البعض، عبر أدوات ووسائل اتصالية حديثة كسرت حاجز الزمان والمكان والحدود ، فأصبحت المعارف والمعلومات عابرة للحدود ،لا تقتصرعلى مجتمع معين ، بل تنتشر بين المجتمعات والأفراد بسبب كثافة وسائل الاتصال وسهولتها

وتوفرها،إلى جانب ذلك لم تكن ظروف الاتصال والتفاعل بين المجتمعات عبر هذه التقنيات المتطورة في وسائل الاتصال ودية فحسب ، بل قد تكون عدائية أيضاً ، إذ أن التطورات المتسارعة في مختلف المجالات ،إلى جانب التطور التقني والمعلوماتي ، ظهرت لنا بعض السلبيات التي تمخضت عن التطور والتقدم، ففي مجال الجريمة خرج الإنسان من مجال الجريمة التقليدية إلى مجال الجرائم المعلوماتية ، الأمر الذي أدى إلى وجود مشكلات اجتماعية واقتصادية وسياسية ، تجاوزت الفرد الواحد لتمس الكيان الدولي.

وقد شهدت السنوات الأخيرة استغلالاً غير مسبوق لشبكات المعلومات والحاسبات الآلية والإنترنت لخدمة الجماعات الإرهابية ، وذلك نظراً لتوافر هذه التقنية وسهولة الحصول عليها وقلة تكاليفها، وإمكانية التخفي والعمل بحرية تامة من خلالها ، كما استخدمت مختلف التقنيات والبرامج المعلوماتية والأنظمة الاتصالية لتسهيل التواصل بين مختلف الفئات والجماعات الإرهابية ومناصريها في جميع أنحاء العالم ،باعتبارها من أكثر وسائل الاتصالأماناوانتشارًا، فقد ساعدت على توجيه الضربات الموجعة لبعض المؤسسات العسكرية والمالية والخدمية- بإلحاق الضرر الكبير أو الشلل التام بأنظمة تلك الجهات (بعزيز، 2012م: 38).

وبسبب تعاظم أهمية أمن المعلومات وأمانها في الآونة الأخيرة ، وتفاقم المهددات وكثرة الاختراقات وتواترها على كل الأصعدة وعلى كافة المستويات من الفرد إلى المؤسسات والوزارات والشركات-فقد بدأت الحكومات والشركات تعي تدريجياً أخطار الجرائم السيبرانية، وأهمية الأمن السيبراني على الأمن الاقتصادي والسياسي للبلد ، وعلى المصالح العامة فقد يبدو الإنترنت جنة لمخترقي الشبكات؛ بسبب ظهورهم عليها ظهورًا فتراضيا، مغفلاً دون اسم، وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السيبرانية، وتدني أخطار ونسب اكتشافها، وصعوبة إثباتها في بعض الدول ، لما تتسم به الجرائم السيبرانية من السرعة التي تتم بها،إذ قد تحدث الأضرار حتى قبل أن تعي الضحية استهدافها.

وتظهر الإحصاءات الصادرة من هيئة الاتصالات وتقنية المعلومات أن عدد مستخدمي الإنترنت في المملكة العربية السعودية لعام (2016) إلى 24 مليون مستخدم، بينما كانت نسبة مستخدمي الإنترنت في عام (2013) يبلغ 17 مليون مستخدم للإنترنت، وهذا يعكس لنا مدى اعتماد الأفراد والمؤسسات على استخدام التقنية؛ لتسهيل التواصل والتعاملات وتسهيل حياة الأفراد في المجتمع السعودي.(هيئة الاتصالات وتقنية المعلومات، التقرير السنوي: 2016).

وهذا يعني الاعتماد الكبير على الإنترنت، وتزايد الثقة في المؤسسات الحكومية والأهلية في منحها الكثير من المعلومات الخاصة والشخصية لأفراد المجتمع؛ لتلبية احتياجاتهم المختلفة وهو من جانب آخر يعكس لنا المخاطر المحتملة التي قد تنتج من تعاملنا واعتمادنا اللا محدود على تكنولوجيا المعلومات، وبالتالي يعد الوعي الاجتماعي بالممارسات والسلوكيات –التي ينبغي أن نتبعها في حياتنا اليومية والعمليةمطلباً أمنياً، يعزز من الحفاظ على الأمن السيبراني في المجتمع السعودي سواءً كان الأمن الفردي أو المجتمعي.

وتتعاظم أهمية هذا المطلب في المؤسسات الحكومية والأهلية التي نثق بها كأفراد في المجتمع، ونودع لديها كافة معلوماتنا الشخصية والحساسة وكافة ممتلكاتنا؛ لتساهم معنا بالحفاظ على أمن هذه المعلومات والممتلكات من الانتهاكات المتنوعة.

موضوع الدراسة

تعد قضية أمن الفضاء السيبراني من القضايا الحساسة التي شغلت الحكومات والأنظمة ومؤسسات الأعمال في شتى أنحاء العالم، إذ مع بروز الممارسات الخطرة والأعمال الإجرامية على شبكة الإنترنت كان لابد من الدول أن تواكب التطور التقني وأن ترفع من التحديات الأمنية والاجتماعية التي باتت تهدد الفضاء السيبراني للمؤسسة والدولة معاً.

ومن جانباً آخر فقد أوضح القران الكريم بوضوح وجوب احترام خصوصية الناس وعدم التجسس عليهم وعلى حياتهم الخاصة ونهى الله عز وجل عن أي شكل من أشكال الفساد أو التسبب في ضرر الآخرين بأي طريقة غير مشروعة قال تعالى : "ولا تبغ الفساد في الأرض إن الله لا يحبالمفسدين"[القصص: 77]، وقوله تعالى :"يا أيها الذين أمنوا اجتنبوا كثيرا من الظن إن بعض الظن إثم، ولا تجسسوا ولا يغتب بعضكم بعضا"[الحجرات: 12].

ولأن مسألة الأمن السيبراني الوطني هي مسألة أمن قومي ، وأمن دولي، تستوجب محاولة فهم أبعادها وكيفية المحافظة على هذا الأمن ، وكيفية تحقيقه ؛ فقد ظهر اهتمام المملكة العربية السعودية بالأنظمة والقوانين والتشريعات لمواجهة خطر الجرائم المعلوماتية، والمحافظة على الأمن السيبراني للمجتمع السعودي من خلال إنشاء هيئة عامة للأمن السيبراني، وإنشاء الاتحاد الخاص بالأمن السيبراني؛ لمواكبة التطور المتسارع في مجال المعلومات والحفاظ على أمنها بجميع الوحدات، سواءً كانوا أفراداً أو مؤسسات حكومية أو أهلية(شلوش، 2018)

فمنذ تأسيس الهيئة الوطنية للأمن السيبراني عام 2017م بأمر ملكي من خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز (حفظه الله)، سجلت الهيئة الوطنية أهم إنجازاتها.

في مارس عام 2019 م عندما صنف الاتحاد الدولي للاتصالات للمملكة العربية السعودية في المرتبة 13 عالمياً والأولى عربياً، من بين 175 دولة من خلال المؤشر العالمي للأمن السيبراني، الذي يتم قياسه كل عامين، وفق معايير معينة في الأمن السيبراني، وما ذلك إلا دليل على أن المملكة بقيادتها الحكيمة تخطو بقوة وثبات نحو تحقيق فضاء سيبراني آمن وموثوق.

ومما لاشك فيه أن اعتماد الدولة ومؤسساتها على تكنولوجيا المعلومات في كافة أعمالها، واستعمال التقنيات الحديثة مرتبط ارتباطاً كبيراً بحدوث مخاطر أنتجتها التقنية، وأصبح هناك دور للوعي المجتمعي في مراقبة وضعيات المخاطر وتهديداتها، فالتطور التكنولوجي السريع، وانتشار التقنيات في المؤسسات والأعمال، واستعمالها بطريقة عقلانية أو غير عقلانية كانت سبباً في إنتاج المخاطر، هذه المخاطر الذي تولدت بفعل التقدم العلمي والتقني تتطلب وعياً اجتماعيا سيبرانياً لدى الأفراد ومستخدمي الإنترنت، خاصة هؤلاء الأفراد العاملين في المؤسسات التي تمتلك بنية معلوماتية حساسة، كالقطاعات المصرفية والعمل البنكي، الذي قد يكون محفوفاً بالعديد من المخاطر لوجود ارتباط بين العمليات الإلكترونية المصرفية وبين أمن المعلومات، والذي يقع على عاتقه مواجهة التحديات والمخاطر المتوقعة على الأنشطة البنكية من التحويل الإلكتروني والعبث بأرصدة العملاء والاحتيال الإلكتروني (ا لعريشي وآخرون، 2015)

بالإضافة إلى طبيعة عمل المؤسسات ونظام كل مؤسسة، فلكل نظام نقطة قوة ونقطة ضعف وثغرات خاصة به، مختلفة عن أنظمة المؤسسات الأخرى، كالقطاع التعليمي يختلف عن القطاع المصرفي في درجة حمايته للموارد البشرية والمالية المرتبطة بتقنية المعلومات والاتصالات.

لذلك تسعى هذه الدراسة لمعرفة مستوى الوعي الاجتماعي بالأمن السيبراني كما يدركه عينة من الخبراء المختصين بالأمن السيبراني في المجتمع السعودي، والتعرف على مدى امتلاكهم لمهارات الحفاظ على الأمن السيبراني، والتصدي لمخاطر الهجمات والجرائم السيبرانية، والتعرف على أهم التدابير الوقائية التي تحد من الهجمات السيبرانية.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في الدور الذي تلعبه تقنية المعلومات الحديثة في حياتنا اليومية وتأثيرها على فكر وسلوك الفرد، حتى أصبحت تمس حياته الشخصية وقضاياه الحساسة؛ فتهدد أمنه الشخصي وتؤثر على الأمن في المجتمع ونظرًا لأن موضوع الأمن السيبراني قد تشكل حديثاً في المجتمع السعودي، ويعد من المواضيع الحيوية والناشطة في الفترة الحالية، فقد ظهرت الحاجة لبحث مدى تشكل الوعي الاجتماعي تجاه الأمن السيبراني لدى الأفراد في المجتمع السعودي، خاصة للعاملين في المؤسسات المختلفة والتي تعتمد على التعاملات الإلكترونية وتقنية المعلومات في تسهيل أعمالها كالقطاعات المصرفية و البنكية.

وتتحددالأهميةالعلمية فيما سوف تضيفه هذه الدراسة من إسهام معرفي في مجال الوعي الاجتماعي، وربطه بالأمن السيبراني، وإثراء للمكتبة المحلية والعربية في هذا المجال، فضلاً عن قلة الدراسات التي تناولت الوعي الاجتماعي وتشكله تجاه الأمن السيبراني، من خلال وجهة نظر العاملين والمختصين بالقطاعات المصرفية والتعليمية ولذلك تأتي هذه الدراسة لسد النقص في هذا المجال.

أهداف الدراسة.

١. التعرف على بداية الاهتمام بمفهوم الأمن السيبراني في المجتمع السعودي.
٢. التعرف على دور القطاع التعليمي والقطاع المصرفي في صناعة الأمن السيبراني في المجتمع السعودي.
٣. التعرف على أهم أنماط الجرائم السيبرانية التي يتعرض لها القطاع المصرفي والتعليمي في المجتمع السعودي.
٤. التعرف على أهم العوامل التي تساعد على تزايد الهجمات السيبرانية على القطاع المصرفي والتعليمي في المجتمع السعودي.
٥. التعرف على أهم التدابير الوقائية ضد الهجمات السيبرانية المتبعة في القطاع المصرفي والتعليمي في المجتمع السعودي.
٦. التعرف على أهم الصعوبات السيبرانية التي يواجهها العاملين المختصين بأمن المعلومات في القطاع المصرفي والتعليمي في المجتمع السعودي.

تساؤلات الدراسة.

١. متى بدأ الاهتمام بصناعة الأمن السيبراني في المجتمع السعودي؟

٢. كيف تساهم القطاعات التعليمية والقطاعات المصرفية في صناعة الأمن السيبراني في المجتمع السعودي؟
٣. ما أكثر أنماط الجرائم السيبرانية التي تتعرض لها القطاعات المصرفية والتعليمية في المجتمع السعودي؟
٤. ما أهم العوامل التي تساعد على تزايد الهجمات السيبرانية على القطاع المصرفي والتعليمي في المجتمع السعودي؟
٥. ما أهم التدابير الوقائية ضد الهجمات السيبرانية المتبعة في القطاع المصرفي والتعليمي في المجتمع السعودي؟
٦. ما أهم الصعوبات السيبرانية التي يواجهها العاملين المختصين في أمن المعلومات في القطاع المصرفي والتعليمي في المجتمع السعودي؟

مفاهيم الدراسة.

تشرح الباحثة في هذه الخطوة من خطوات البحث العلمي عدداً من المفاهيم الأساسية في حقل أمن المعلومات، وحقل علم الاجتماع، وتطرح مفاهيم أساسية أخرى قد تتطرق لها الدراسة في بعض الفصول، وتُعد هذه الخطوة مهمة في الدراسة؛ لأنها تمهد للقارئ للتعرف على الأفكار الواردة في هذه الدراسة.

أولاً: مفهوم أمن المعلومات :information security

لقد تعددت التعاريف الرسمية لأمن المعلومات وفيما يأتي تعريف أمن المعلومات المتوافق مع اتجاهات هذه الدراسة، أمن المعلومات هو ممارسة العمل الذي يتمثل في حماية المعلومات الخاصة من السرقة أو الإفشاء أو التخريب وإدخالها في وضع الأمان والمحافظة عليها وتقتضي حماية المعلومات في هذا التعريف حماية محيطها ومحيط مالكها أيضًا. (الخالد، 2018: 15)

وهناك فرقٌ بين أمن المعلومات وأمان المعلومات وكما تم تعريف أمن المعلومات في ممارسة عمل لحماية المعلومات الخاصة، فإن أمان المعلومات information safety فهو الحالة أو الوضع التي تدخل فيها المعلومات الخاصة بعد اتخاذ إجراءات أمن المعلومات، أي بعد حمايتها من السرقة أو الإفشاء أو التخريب، واتخاذ الإجراءات المستمرة لضمان أمان هذه المعلومات والتعامل مع المستجدات.

ثانياً: مفهوم الأمن السيبراني Cybersecurity

يمثل الأمن السيبراني تحدياً يتطور على الدوام، ومن اللازم متابعته باستمرار؛ نظراً للتغير الدائم في طبيعة تكنولوجيا المعلومات والاتصالات، ويمكن تعريف الأمن السيبراني بأنه الأمن الذي يعني بالحفاظ على أمن المعلومات وشبكات وأجهزة الحاسب الآلي (مختار، 2015: 5).

وقد قدمت وزارة الدفاع في الولايات المتحدة الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني، حيث اعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادية من مختلف الجرائم والهجمات، التخريب، التجسس والحوادث " (صائغ، 2018: 15)

كما يمكن تعريف الأمن السيبراني بأنه: تلك الطرق التي تستهدف كشف ومنع الهجمات على أي نظام حاسوبي والمعلومات المتضمنة فيه أو الوصول غير المصرح له، ويستهدف الأمن السيبراني حماية البيانات أو أي شكل من الأصول الرقمية المخزنة في حاسوب لأي جهة أو في أي جهاز يحتوي على ذاكرة رقمية (علي، 2017: 24).

التعريف الإجرائي

هو تلك الممارسات والإجراءات والسلوكيات التي يقوم بها العاملون في القطاعات المصرفية والتعليمية في المجتمع السعودي على أجهزة الحاسب الآلي؛ لحماية البيانات والمعلومات ذات الأهمية بجميع التعاملات والأنشطة الإلكترونية.

ثالثاً: مفهوم الوعي المعلوماتي Information Awareness

تعددت التعاريف الخاصة بالوعي المعلوماتي تبعاً لتعدد المهتمين بهذا الموضوع، فقد ورد بالنتاج الفكري عدة تعاريف صادرة من منظمات وهيئات معلوماتية، لكنها تنبثق جميعها من تعريف الوارد من اللجنة الرئاسية للوعي المعلوماتي بجمعية المكتبات الأمريكية، بأنه: القدرة على تحديد وقت الاحتياج للمعلومات والقدرة على تحديد مكان هذه المعلومات ثم تقييمها واستخدامها بكفاية وفاعلية.

كما عرفت منظمة اليونسكو الوعي المعلوماتي بأنه: تحديد الحاجات والاهتمامات المعلوماتية والقدرة على تحديد مكانها وتقييمها وتنظيمها، وإعدادها بكفاءة واستخدامها، والاتصال بالمعلومات لمعالجة القضايا والمشاكل.

التعريف الإجرائي: إدراك المبحوثين لأهمية المعلومة وكيفية استخدامها والحفاظ عليها وتقييمها في القطاعات المصرفية والتعليمية في المجتمع السعودي.

رابعاً: مفهوم الجرائم السيبرانية Cyber Crimes

تعتبر الجريمة الإلكترونية هي: جميع الأفعال المخالفة للتشريع الإسلامي والتي ترتكب بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، وتُعرف الجريمة السيبرانية بأنها: أي جريمة تشتمل على جهاز حاسوب وشبكة اتصال، وهي جرائم ترتكب ضد الأفراد والجماعات من قبل أفراد لديهم دافع إجرامي لتعمد إيذاء الضحايا من خلال تكنولوجيا المعلومات والاتصالات الحديثة.

سادساً: مفهوم الوعي الاجتماعي Social awareness

تناولت العلوم الإنسانية عبر التاريخ مفهوم الوعي بالشرح والتحليل؛ لما لهذا المفهوم من أهمية بالغة؛ كونه يمثل عملية حيوية يقوم بتنميتها الفرد حسب بيئته الاجتماعية، وقد حظي هذا المفهوم بالاهتمام لدى الكثير من العلماء والمفكرين والباحثين، أمثال: كارل ماركس، وجورج ميد، وناقشوا هذا المفهوم كلاً حسب اهتمامه.

والوعي يعني: معرفة الأشياء على نحو مستمر، وفي اللغة الإنجليزية يعني: إدراك الفرد لنفسه ولمن حوله.

وفي أوائل القرن التاسع عشر ظهر علم النفس إلى الوجود كعلم باسم (علم الوعي)، مستخدماً مصطلح الوعي ليشمل: كل الإحساسات والصور الذهنية والأفكار، والرغبات، والعواطف أي العمليات العقلية للإنسان.

ويقدم علماء الاجتماع تعريفًا للوعي يحدد بأنه: أسلوب إدراك كل جماعة للواقع الاجتماعي، بما يشتمل عليه من علاقات ونظم، وفهمهم لما يدور فيه من أحداث وتقويمهم لها، وردود أفعاله اتجاهها (الفردي، 2015: 41)

يرى العالم (ميد) أن الوعي ينشأ نتيجة الفعل الاجتماعي، حيث تساعد عملية التواصل الاجتماعي في زيادة مقدرة الفرد على أن يعي نفسه، بل وأن يرى نفسه من منطق الآخرين، ومن خلال نظر (ميد) نجد أن هناك مستويان للوعي:

أولهما: الوعي الفردي، أي وعي الإنسان الفرد.

ثانيهما: الوعي الاجتماعي كظاهرة ذات طابع جماهيري، وهو ما يهمنا في هذه الدراسة وما تسعى إليه الدراسة هو معرفة الوعي الاجتماعي نحو الأمن السيبراني في المجتمع السعودي.

إذا يعرف الوعي الاجتماعي بأنه: اتجاه عقلي انعكاسي يمكن الفرد من الوعي بذاته وبالبيئة المحيطة به، بدرجات متفاوتة من الوضوح والتعقيد ويتضمن ذلك وعي الفرد بالوظائف العقلية والجسمية، ووعيه بالأشياء والعالم الخارجي وإدراكه لذاته فردياً، وكعضو في جماعة (غيث، 2006: 79)

التعريف الإجرائي:

إدراك المبحوثين، وهم: العاملون المختصون في أمن المعلومات في العمل المصرفي والتعليمي، وانتباههم لمجموعة القواعد والممارسات التي يقومون بها أثناء عملهم؛ للحفاظ على الأمن السيبراني للمؤسسة التي يعملون بها.

سابعاً: مجتمع المخاطرة Risk Society

وهو ذلك المجتمع الذي يمر بتغيرات تقنية أثناء تقدمه المتسارع، ويجلب معه أنواعاً جديدة من المخاطر التي يجب على الانسان أن يواجهها أو يتكيف معها، وهي سلسلة من التغيرات المترابطة والمتداخلة في حياتنا الاجتماعية المعاصرة.

ويرى (أو لريخ بك) عالم الاجتماع الألماني أن جانباً مهماً من مجتمع المخاطرة يتمثل في: الأخطار التي تنتشر وتبرز بصرف النظر عن الاعتبارات المكانية والزمانية والاجتماعية، والتي لها آثار شخصية وعالمية في الوقت نفسه (بيك، 2009).

إجراءات الدراسة:

نوع الدراسة

تعد هذه الدراسة دراسةوصفيةتهدفإلى دراسة المشكلة أو الظاهرة كما توجد في الواقع، ويعبر عنها بتعبير كمي أو كيفي، وهذا يعني أن البحث الوصفي يهتم بدراسة حاضر الظواهر والأحداث ويهتم بوصف نشاطات وعمليات وأشخاص، ويمكن أن يهتم بالعلاقات السائدة بين الظواهر الجارية ويشمل محاولات للتنبؤ بوقائع في المستقبل.

منهج الدراسة

تختلف المناهج باختلاف الظواهر والمشكلات المدروسة وما يصلح منها لدراسة ظاهرة معينة قد لا يصلح لدراسة ظاهرة أخرى ولكن هذا لا ينفي بشكل مطلق إمكانية دراسة ظاهرة ما باستخدام أكثر من أسلوب أو منهج علمي (الزيباري، 2011: 56).

وفي هذه الدراسة طبقت الباحثة المنهج الوصفي، وهو يعتبر من أشهر مناهج البحث وأكثرها استخداماً في الدراسات الوصفية خاصة، ويوفر الكثير من البيانات والمعلومات عن موضوع الدراسة.

مجتمع الدراسة

ويتكون مجتمع الدراسة من جميع الأفراد العاملين في القطاع المصرفي والمختصين بإدارة أمن المعلومات في المصرف، والأفراد العاملين بإدارة أمن المعلومات في القطاع التعليمي والمتمثل بالجامعات الحكومية في مدينة الرياض.

وقد تم اختيار جميع مفردات مجتمع الدراسة من الأفراد العاملين في إدارة أمن المعلومات في البنوك السعودية المحلية والجامعات السعودية الحكومية في مدينة الرياض.

وفيما يخص عينة الخبراء المتخصصين في الأمن السيبراني وجهت الباحثة خطاب رسمياً من جامعة الملك سعود إلى هيئة الاتصالات وتقنية المعلومات باعتبارها منصة رسمية حكومية حاضنة لمتخصصين في الأمن السيبراني وقد تم تزويد الباحثة بعينة من الخبراء المتخصصين في الأمن السيبراني والبالغ عددهم (5) مفردات وقد تم اجراء المقابلة معهم لاستيفاء الحقائق التي تصف موضوع الدراسة وتجيب على تساؤلاتها.

عينة الدراسة

تكونت عينة الدراسة من الأفراد العاملين في القطاع المصرفي المختصين في إدارة أمن المعلومات في العمل المصرفي في البنوك السعودية المحلية في مدينة الرياض والأفراد العاملين المختصين في إدارة أمن المعلومات في القطاع التعليمي المتمثل في الجامعات الحكومية في مدينة الرياض.

بالإضافة إلى عينة الخبراء المتخصصين في الأمن السيبراني في هيئة الاتصالات وتقنية المعلومات.

حدود الدراسة

لضبط مسار الدراسة ورسم المعالم الأساسية لها تقيدت بالحدود التالية:

- **أولاً: الحدود البشرية:** تتمثل الحدود البشرية للدراسة في: مجموعة العاملين في القطاع المصرفي المختصين في إدارة امن المعلومات والتعاملات الإلكترونية بالعمل المصرفي في مدينة الرياض، والعاملين في القطاع التعليمي، المتمثل: بالجامعات الحكومية في مدينة الرياض وهم الموظفين المختصين بإدارة أمن المعلومات والتعاملات الإلكترونية فقط.
- **عينة الخبراء المتخصصين بالأمن السيبراني في هيئة الاتصالات وتقنية المعلومات.**
- **ثانياً: الحدود الزمنية:** تتمثل الحدود الزمنية في الفترة اللازمة لإجراء الدراسة والتي امتدت الحدود الزمنية لهذه الدراسة خلال الفترة الممتدة من شهر شعبان لعام 1440هـ ابتداءً من اختيار عنوان الدراسة ومجالاتها ووصولاً إلى تفريغ البيانات وتحليلها وقد استغرق جمع البيانات 7 أشهر من 1442/2/11 إلى 1442/7/25هـ.
- **ثالثاً: الحدود المكانية:** طُبقت الدراسة بإدارات أمن المعلومات في البنوك السعودية المحلية في مدينة الرياض، بالإضافة إلى إدارات أمن المعلومات والتعاملات الإلكترونية بالجامعات السعودية الحكومية في مدينة الرياض.

أداة الدراسة

استخدمت الباحثة في هذه الدراسة نوعين من أدوات جمع البيانات على حسب العينة المدروسة، فقد طبقت أداة الاستبيان الإلكتروني على عينة العاملين المختصين بأمن المعلومات، كما استخدمت أداة المقابلة على عينة من الخبراء المختصين بالأمن السيبراني.

وتهدف مقابلةالخبراءإلى التركيز على التجارب الذاتية للأشخاص "بوصفه خبير "،وقد تم إجراء مقابلة علمية مع عينة من الخبراء في مجال الأمن السيبراني وذلك لاستيفاء المعلومات حول عدة نقاط حول الأمن السيبراني وأهم اللوائح والأنظمة التي تتبعها لحماية الأمنالسيبراني والبرامج التوعوية والتثقيفية التي تقيمها لتعزيز الوعي الاجتماعي بمفهوم الأمن السيبراني لدى العاملين تحت مظلتها.

وقد اشتمل دليل المقابلة على مجموعة من الأسئلة المباشرة المفتوحة والتي تتيح للخبير فرصة الإجابة المفتوحة والاسهاب بالموضوع حسب كل سؤال يعكس تساؤلات الدراسة.

نتائج الدراسة.

توصلت هذه الدراسة إلى مجموعة من النتائج وهي كما يلي حسب تساؤلات الدراسة:

إجابة التساؤل الأول: متى بدأ الاهتمام بصناعة الأمن السيبراني في المجتمع السعودي؟

اتفق الخبراء كلاً من (ع، ش) و(ف، د) على أن هناك نوعين من الاهتمام بالأمن السيبراني على مستوى المملكة العربية السعودية، حيث صنفوا الاهتمام على المستوى الحكومي وآخر على المستوى الشعبي، وقد كان الاهتمام الحكومي من بدايات عام 2012م وتحت مسمى الأمن الإلكتروني أو الأمن المعلوماتي حيث تم إنشاء مركز الأمن الإلكتروني التابع لوزارة الداخلية آنذاك، وهو مركز سعودي يُعنى بحماية الفضاء الإلكتروني السعودي من أي تهديدات وهجمات، كما يختص بمعالجة الجرائم المعلوماتية التي يقع الأفراد ضحايا لها خاصة بعد انتشار الاختراقات والانتهاكات المعلوماتية، وحدوث بعض الجرائم الإلكترونية بعد دخول الأجهزة الذكية إلى المجتمع السعودي.

وعلى صعيد الاهتمام الشعبي أو اهتمام الأفراد بالأمن السيبراني عموماً باختلاف مسمياته في الفترات السابقة يرى الخبيرين (ع، ش) و(ف، د) أن تأخر الاهتمام الشعبي بهذه القضية طبيعي بسبب حداثة التقنية، وجدية المجال على المجتمع السعودي، وقد ساعد من معرفة الأفراد بهذا المجال هو سرعة انتشار الأجهزة الذكية وما تحمله من تطبيقات ومنصات إلكترونية والتي كانت تساهم بشكل كبير في انتشار المعلومة.

ويرى الخبير (ف، د) أن هذه المنصات الرسمية والتطبيقات المعلوماتية في الأجهزة الذكية بتوجيه من الاهتمام الحكومي مكنت الخبراء والمختصين بمجال أمن المعلومات والأمن السيبراني من توعية المجتمع حول مفهوم الأمن السيبراني وأبعاده وأهم الأساليب التي ينتهجها المجرمين لإيقاع الأفراد كضحايا للجريمة السيبرانية.

ويرى الخبير (م ،ع) و(إ، ص) أن بداية صناعة الأمن السيبراني في المجتمع السعودي بدأت بعد دخول الإنترنت بشكل واسع إلى المجتمع وانطلاق شبكاته، وسهولة الحصول عليه الأمر الذي جعل الأجهزة الذكية تنتشر وينخرط الأفراد في المجتمع بالتواصل مع المجتمعات الخارجية، والدخول إلى المنتديات والمواقع المختلفة، الأمر الذي أدى إلى إنتشار موجة من الاختراقات على بعض المؤسسات الحكومية، مما جعل المملكة العربية السعودية تعمل على تعزيز وتحصين الأمن السيبراني للمجتمع السعودي بإنشاء واستحداث مختلف الهيئات والمراكز والكليات المتخصصة بتأهيل كوادر وطنية لتشغيلهم في هذه الهيئات و لرفع مستوى الوعي لدى أفراد المجتمع السعودي حول الأمن السيبراني .

ويرى الخبير (ف،د) أن بعد إنتشار فايروس شمعون والذي ضرب بعض المؤسسات الحكومية والخاصة في المجتمع السعودي عام 2017م، والذي كان يهدف إلى اختراق البيانات وتدميرها إلكترونيا، وألحق بعض الأضرار الطفيفة على بعض المؤسسات الحكومية؛ نتيجة لعدم وجو أمن معلوماتي متكامل يحقق الحصانة اللازمة للجهات الرسمية في المجتمع السعودي صدر من المقام السامي المرسوم الملكي الذي يقتضي بإنشاء هيئة حكومية متخصصة في الأمن السيبراني مهتمة في شؤونه لها شخصيتها المستقلة ومرتبطة مباشرة بالملك سلمان بن عبدالعزيز لما لهذه الهيئة من أهمية كبيرة ومكانة حساسة في المجتمع السعودي والتي تأسست عام 2017 م، ووضعت لها اختصاصاتها ومهامها وأهم البرامج التي تعنى بتفعيلها على مستوى المجتمع السعودي .

وبتوجيه من حكومة المملكة العربية السعودية اتفقت آراء الخبراء حول أن التوجه الحكومي والاهتمام الرسمي بموضوع الأمن السيبراني، جعل أفراد المجتمع السعودي يحاولون معرفة خفايا هذا المجال والتعرف عليه من خلال القراءة عنه، والاطلاع على كيفية حماية الأمن السيبراني للفرد والمجتمع على حد سواء.

إجابة التساؤل الثاني: كيف تساهم القطاعات التعليمية والقطاعات المصرفية في صناعة الأمن السيبراني في المجتمع السعودي؟

اتفق الخبراء جميعهم كل من (ع،ش)و(ف،د) و(م،ض) و(م، ع) (إ،ص) أن اهتمام القطاع التعليمي بمجال الأمن السيبراني بدأ متأخراً وقد يرجع هذا التأخر إلى جدية مجال الأمن السيبراني على وجه التحديد ليس على المجتمع السعودي فقط بل على المستوى الدولي أيضاً يواجه مجال الأمن السيبراني في كل دولة تحدي كبير في الحفاظ على الأمن السيبراني للقطاعات الحكومية أو الأهلية في المجتمع ، وذكروا أن أمام التعليم فرصة كبيرة جداً في استحداث التخصصات الدقيقة في مجال الأمن السيبراني من خلال الجامعات أو الكليات المتخصصة بعلوم الحاسب الآلي.

وتفسر الباحثة اقوال الخبراء حول تأخر القطاع التعليمي في الاهتمام في بقضية الأمن السيبراني لعدة أسباب، كما تراها الباحثة كون المجال حديث وتخصص دقيق من تخصصات الحاسب الآلي لذلك تبعه تأخر في استحداث التخصصات الجامعية والمناهج العلمية والعملية في هذا المجال وقد يرجع إلى ندرة المتخصصين في الأمن المعلوماتي بالقطاع التعليمي والذي يقع على عاتقهم صنع وتصميم المبادرات التي تهدف إلى انشاء التخصصات الحيوية في مجال الأمن السيبراني كما قد يرجع آلية تقديم الخدمات

التعليمية فقد كانت الخدمات التعليمية تقدم بشكل مباشر وبالطريقة التقليدية ولا تعتمد اعتمادا كليا على التقنية في التعليم وتأخر دخول الخدمات الإلكترونية في إنجاز المهام التعليمية.

وترى الباحثة أن القطاع التعليمي يسير ببطء حول توعية الأفراد الذين ينتمون لهذا القطاع والذين يشكلون الشريحة العظمى من الأفراد في المملكة العربية السعودية وترى الباحثة أنه من الضروري نشر البرامج التثقيفية على صعيد العاملين بالقطاع والمستفيدين منه من أولياء أمور أو طلاب وضرورة عقد الشراكات المجتمعية للحملات التوعوية الواسعة اتجاه موضوع الأمن السيبراني.

ووصف الخبراء حول دور القطاع المصرفي في موضوع الأمن السيبراني بأن القطاع (ناضج جداً) في مسألة الحفاظ على الأمن السيبراني إذا يعتبر من أكثر القطاعات تحصيناً في الحفاظ على الأمن السيبراني ويرجع ذلك إلى إجراءات المنصة الرسمية التي تتبعها البنوك السعودية وهو البنك المركزي السعودي (ساما) حيث وصفوا إجراءاته بالتخصصية الدقيقة والمتجددة والتي تخضع للتحديث المستمر للاطلاع على كل ما هو جديد في قضية الحفاظ على الأمن السيبراني.

وتساءل الخبراء حول سبب ربط الباحثة القطاع التعليمي مع القطاع المصرفي رغم اختلاف القطاعين كماً وكيفاً وقد فسرت الباحثة لهم مبررات اختيار القطاعين يرجع إلى أنها من أهم القطاعات الموجودة على مستوى الوطن كما أن القطاع المصرفي يُعنى بحماية الأمن السيبراني لأموال الأفراد داخل المجتمع السعودي كذلك القطاع التعليمي يُعنى بحماية العقول وتنشئة هؤلاء الأفراد على ضرورة حماية معلوماتهم الشخصية وتعليمهم كيفية التعامل مع التقنيات المتجددة وكيفية استخدامها.

وبالتالي يهتم كلا القطاعين القطاع المصرفي والقطاع التعليمي رغم اختلاف اهتماماتهم اتجاه الأمن السيبراني في مؤسساتهم إلا أنهم يشتركون في هدف واحد وهو حماية العقل وحماية المال للفرد والمجتمع.

إجابة التساؤل الثالث: هل لك أن تصف لي أكثر أنماط الجرائم السيبرانية انتشارا في القطاع المصرفي والقطاع التعليمي؟

اتفق جميع الخبراء على أن جريمة النصب والاحتيال باختلاف مسمياتهم لتلك الجريمة (كالاحتيال الإلكتروني، اختلاس الأموال، المكالمات الانتحالية، رسائل التصيد) هي من أكثر الجرائم السيبرانية انتشاراً في المجتمع السعودي ويرجعون سبب انتشارها إلى قلة وعي الأفراد في التعامل مع القضايا التي تمس المعلومات الشخصية والمالية مع الآخرين.

وتفسر الباحثة سبب آخر لانتشار جرائم النصب والاحتيال على صعيد الأفراد بسبب تعدد وتجدد الأساليب الإجرامية والانتحالية التي يقوم بها المجرم في إيقاع الضحايا ضمن الهدف والتي يقوم بها الهاكرز باستهداف العملاء حسب أي قطاع يستهدفه بطلب معلومات شخصية من المستخدم بصفته موظف ينتمي لهذا القطاع ويتعامل مع الضحية بغرض تحديث البيانات أو الفوز بجائزة معينة ويتم استغلالها لأغراض أخرى.

وأشار الخبير (إ، ص) إلى أن اسلوب الهندسة الاجتماعية من أكثر الأساليب انتشاراً حيث يعتمد على مجموعة من الحيل لخداع الناس وجعلهم يقومون بعمل ما يطلب منهم أو يفصحون عن معلومات سرية أو شخصية وتستخدم هذه المعلومات لأغراض متعددة من قبل المجرم.

إجابة التساؤل الرابع: ماهي أهم العوامل التي تساعد على تزايد الهجمات السيبرانية في القطاع المصرفي أو القطاع التعليمي في المجتمع السعودي؟

يذكر الخبير(ف،د) و(م، ع) أن هناك عوامل تخص المؤسسات التابعة للقطاع وهناك عوامل تخص الأفراد الذين ينتمون إلى القطاع كمنسوبين أو كمستفيدين من خدمات القطاع وهي التي تزيد من فرصة حدوث الهجمات السيبرانية، فالعوامل التي تختص بالمؤسسات التي تكون تابعة للقطاع تتمثل في المقام الأول حيوية القطاع ومدى قوة جذبه وحساسية مكانته في المجتمع هي التي تجعل الهاكرز أو المهاجمين يستغلون هذه المكانة في شن التهديدات السيبرانية واستهداف النظام المؤسسي بشكل كامل وأيضاً ضعف برامج الحماية المستخدمة في معالجة المعلومات الخاصة بالعملاء والمستفيدين.

أما عن العوامل التي تخص المنتمين للقطاع من عاملين في القطاع أو مستفيدين فهي تشكل الحلقة الأضعف في مسألة الحفاظ على الأمن السيبراني في القطاع فوجود عاملين ينقصهم الوعي حول الإجراءات التي يجب أن تتبع في أداء وتقديم الخدمات الإلكترونية قد يزيد من فرصة حدوث الهجمات على القطاع كما ذكرها الخبير (م، ع) الدخول إلى مواقع مشبوهة من الحاسب الآلي التابع للعمل أو فتح الروابط الملغمة أو الدخول إلى مواقع تحمل الكثير من الفيروسات وعلى صعيد المستفيدين من الخدمة قد يؤدي ضعف الوعي لدى المستفيد إلى حدوث الهجمات السيبرانية مثل إفشاء المعلومات الشخصية ومشاركتها المنتحلين بلا وعي.

وتتفق الباحثة مع رأي الخبير (إ، ص) الذي يرى أن من أهم العوامل التي تزيد من الهجمات السيبرانية على القطاعات هي العالم الرقمي الكبير الواسع الانتشار وتوسع الخدمات الإلكترونية والمنصات الرسمية التابعة للقطاع يجعل من أمر الضبط والحماية صعب في حماية الأمن السيبراني.

إجابة التساؤل الخامس: ما أهم الصعوبات السيبرانية التي تواجه العاملين في القطاع التعليمي والقطاع المصرفي؟

يؤكد الخبير (د، ض) على عنصر الوعي الاجتماعي لدى الأفراد في المجتمع السعودي ويتفق معه جميع الخبراء حول هذا الرأي بأن ضعف الوعي لدى الفرد يُسهم بإلحاق أضرار جسيمة على صعيد الفرد نفسه والمجتمع المحيط به فإفشاء المعلومات الشخصية ومشاركتها غير المتخصصين الرسميين في تقديم الخدمات هي الصعوبة الحقيقة في قضية الأمن السيبراني.

ويُشير الخبير (ف، د) أن تعدد الأنظمة التي يستخدمها القطاع التعليمي بشكل خاص يمثل تحدي كبير وصعوبة يواجهها في الحفاظ على الأمن السيبراني للقطاع، فالمنصات الكثيرة والتطبيقات المختلفة التي يستخدمها القطاع التعليمي لتحقيق أهدافه التعليمية يمثل عائق يصعب التغلب عليه.

أما في القطاع المصرفي يرى جميع الخبراء أن الصعوبة الحقيقة تكمن عند المستخدم والعميل في طريقة التعامل مع الاتصالات الانتحالية وأسلوب الهندسة الاجتماعية وطرق الاختراق المتجددة والتي تستهدف الفرد في المقام الأول.

إجابة السؤال السادس: ماهي أهم التدابير الوقائية التي يجب أن يتبعها العاملين المختصين بأمن المعلومات في القطاع المصرفي والقطاع التعليمي؟

يرى الخبير (ع، ش) أن هناك نوعين من التدابير التي يجب أن تتم في كل القطاعات فهناك تدابير وقائية تتم على مستوى المسئولين في القطاع ومتخذي القرار بالقطاع وهناك تدابير تتم على مستوى الجمهور سواء الجمهور التابع للقطاع أو الأفراد بالمجتمع بشكلٍ عام.

فالتدابير الوقائية على مستوى متخذي القرار في القطاع يواجه غالباً المسئولين عن الحفاظ على الأمن السيبراني في القطاع صعوبة في إقناع متخذي القرار في القطاع نفسه في عدة أمور تختص بإدارة الأمن السيبراني في القطاع منها: الاعتمادات المالية ووضع ميزانية مقترحة لحماية الأمن السيبراني للقطاع وهي معروفة بأنها باهظة الثمن ومكلفة ولكن تحقق مستوى قوي من حماية الأمن السيبراني في القطاع

فغالباً يواجهون صعوبة في إقناع متخذي القرار حول المبالغ المالية اللازمة لإدارة الأمن السيبراني لأنها حسب رأي الخبير غير مرئية أمام الجميع ولكن يتضح أهميتها وقيمتها عند محاولة الهجوم والاختراق للقطاع.

ويضيف الخبير (ف، د) أن إتباع السياسات المفروضة من قبل القطاع على الموظفين يساهم أيضاً من تقليل فرض الهجمات السيبرانية باستخدام كلمات مرور قوية، تجنب دخول المواقع المشبوهة، تجنب تحميل أي ملفات دون فحصها من الفيروسات التي تنتقل إلى الجهاز.

وترى الباحثة من خلال آراء عينة الدراسة وآراء الخبراء المختصين حول هذا المحور التأكيد على مراجعة السياسات المرتبطة بالأمن السيبراني بشكل دوري والعمل على تحديثها بشكل مستمر لاكتشاف الثغرات التي قد توجد بين كل تحديث وآخر وإصلاح الأخطاء.

وتتفق الباحثة حول رأي جميع الخبراء بأهمية توعية المستخدم النهائي والمستفيد الأول للخدمات الإلكترونية والتي يُطلقها القطاع قبل تنفيذ الخدمة عبر حملات توعوية ونشرات تثقيفية بأساليب جاذبة لاطلاع المستخدم على المعلومة.

ولما لهذا الإجراء من أهمية كبيرة في ظل تنامي المكتشفات العلمية المرتبطة بالتقنية وتزايد الحاجة إلى المعلومات وسرعة الحصول عليها لدرجة اعتماد الحكومات ومؤسساتها على التقنية ومعطياتها في إتمام الأعمال الرسمية للأفراد وتسهيل العمل على الأفراد والمؤسسات يبرز لدينا بشكل واضح من خلال هذه الدراسة على أهمية الوعي الاجتماعي للأفراد في المجتمع السعودي خاصة أن الكثير من الجرائم المعلوماتية والهجمات السيبرانية قد وقعت بسبب أخطاء بشرية غير مقصودة في التعامل مع التقنية.

ثانياً: مناقشة النتائج في ضوء النظريات والدراسات السابقة

حسب نظرية مجتمع المخاطرة للعالم أولو ريخ بك يرى أن مجتمع المخاطرة هو ذلك المجتمع الذي يُعايش حالة من انتشار القلق والمشاكل نتيجة التقدم الهائل في التقنية، فهو يفسر سلوكيات الأفراد في هذا المجتمع وطريقة تفاعلهم مع الأحداث الناتجة من هذا التقدم هو التفكير ملياً بالأحداث ومحاولة إدراك المخاطر الجديدة التي أنتجتها هذه التغيرات التقنية.

ومن خلال النتائج التي توصلت إليها هذه الدراسة نجد أن الأفراد العاملين المختصين بأمن المعلومات في القطاع التعليمي والقطاع المصرفي يرون أن من أبرز أولويات الفرد أثناء التعامل مع التقنية

ولاسيما في مجال الأمن السيبراني هو أن يكون أكثر تمكنناً وإدراكاً للمخاطر التي يمكن أن تظهر له في الفضاء السيبراني وهذا ما أكدته نتائج عينة الخبراء المختصين بأمن المعلومات حول أهمية ارتفاع مستوى الوعي الاجتماعي للأفراد العاملين والمنتمين لمختلف القطاعات.

ويرى أولو ريخ بيك أن النمو التقني والمعلوماتي يساهم في ولادة مخاطر وإمكانيات قد تُعرض العالم لخطر لا سابق لاتساعه، وقد توصلت هذه الدراسة إلى نتيجة تؤكد هذه الفكرة، فأن من أبرز وأهم العوامل التي تزيد من حدوث الهجمات والمخاطر السيبرانية هي حيوية مجال أمن المعلومات والتجدد المستمر في التقنيات الأمر الذي يقابله ابتكار في أساليب الهجمات السيبرانية الذي قد تلحق مختلف الأضرار في القطاعات.

واستعانت الباحثة في تفسير هذه الدراسة من منظور الانعكاسية الاجتماعية للعالم (أنتوني غيدنز) الذي تأثر تأثراً واضحاً بمفهوم المخاطرة لدى العالم أولو ريخ بك فنجد أنه يضيف مفهوماً آخر للمخاطرة وهو مفهوم الثقة والذي يقصد به كيف لنا نحن الأفراد أن نعقد آمالنا ونعطي ثقتنا على أنساق مجردة لا نعرفها معرفةً وثيقة ولكن تؤثر في حياتنا تأثيراً مباشراً، حيث أن الثقة والمخاطرة مفهومان مرتبطان ارتباطاً وثيقاً ببعضهما البعض، ونجد أن هذه الدراسة توصلت إلى نتيجة تفسر هذه النظرية والذي تتمثل حول اتفاق وجهة نظر العاملين المختصين في أمن المعلومات في القطاع المصرفي والقطاع التعليمي وعينة الخبراء حول أكثر أنماط الجرائم السيبرانية انتشارا والتي ذُكر أبرزها جرائم النصب والاحتيال والتي تقوم على أسلوب الهندسة الاجتماعية.

مما يجعل عنصر الثقة لدى الأفراد يهتز بسبب سلوكيات وأساليب إجرامية تنتحل السمات الرسمية للقطاعات لاستدراج المعلومات المهمة من الفرد واستخدامها لأغراض أخرى.

قائمة المراجع

أولاً: الكتب العلمية

١. دخيل، عز الدين (2009) المناهج وتقنيات البحث في علم الاجتماع، الطبعة الأولى، مركز النشر الجامعي.

٢. الزيباري، طاهر حسو (2011) أساليب البحث العلمي في علم الاجتماع، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر والتوزيع،بيروت.

٣. الشايع، خالد سعد (2019) الأمن السيبراني مفهومه وخصائصه وسياساته، الدار العالمية، الطبعة الأولى، مصر.

٤. العساف،صالح. (1995) المدخل إلىإلى البحث في العلوم السلوكية، الطبعة الأولى،الرياض: مكتبةالعبيكان.

٥. علي، إيهاب عبد الرحيم (2017) أمن المعلومات الصحية، مجلة التقدم العلمي، الكويت (99) :1-10

٦. الغندور، محمد جلال. (2015) البحث العلمي بين النظرية والتطبيق.القاهرة: دار الجوهرة.

٧. الحسن، احسان محمد. (2015) النظريات الاجتماعية المتقدمة دراسة تحليلية في النظريات الاجتماعية المعاصرة، دار وائل للنشر، عمان.

٨. دودين حمزة محمد. (2018) التحليل الإحصائي المتقدم للبيانات باستخدام spss، دار المسيرة للنشر والتوزيع، عمان.

٩. غيدنز، أنتوني (2005) علم الاجتماع، ترجمة فايز الصياغ، المنظمة العربية للترجمة، الطبعة الأولى، بيروت.

ثانياً: المجلات العلمية

١٠. مختار، محمد (2015) cyber securityهل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟، اتجاهات الأحداث، مفاهيم المستقبل (67)

١١. بيك، أو لريخ (2009) مجتمع المخاطرة، المكتبة الشرقية، ترجمة كتورة، الطبعة الأولى.

١٢. جناوي،عبد العزيز (2018) قراءةفيسوسيولوجيامخاطرالحداثةالانعكاسية،مجلةدراساتوأبحاث،المجل د30، عدد30

١٣. جبور،منالأشقر (2017)

السيبرانيةهاجسالعصر،مجلةالمكتباتوالمعلوماتوالتوثيقفيالعالمالعربي،المجلدوالعدد5.

١٤. المقصودي،محمدبنأحمد (2017)

الأمنالسيبرانيوالجهودالدوليةلمكافحةالجرائمعابرةالقارات،مجلةالأمنوالحياة،جامعةنايفالعربيةللعلومالأمنية ،المجلد37،العدد427.

١٥. شلوش،نورة (2018)

القرصنةالإلكترونيةفيالفضاءالسيبراني،التهديدالمتصاعدلأمنالدول،مجلةمركزبابللدراساتالإنسانية، جامعةبابل،العراقالمجل د8 العدد 2

١٦. العتيبي،فيصلعبد الله (2017)

برامجالتوطينبالقطاعالخاصفيدولمجلسالتعاونمراجعةنقديةمنمنظورالاختيارالعقلانيحالةالمملكةالعربيةالسعو دية،المركزالعربيللأبحاثودراسةالسياسات،مجلةعمرانللعلومالاجتماعية.

١٧. البار،عدنانوالمرجي،خالد (2018) أمنالمعلوماتوالأمنالسيبراني.

١٨. صائغ،وفاءحسنعبد الوهاب(2018)

وعيأفرادالأسرةبمفهومالأمنالسيبرانيوعلاقتهباحتياطاتهمالأمنيةمنالجرائمالإلكترونية،المجلةالعربيةللعلوما لاجتماعية،المؤسسةالعربيةللاستشاراتالعلميةوتنميةالمواردالبشريةالعدد 14 المجلد 3.

ثالثاً: الرسائل العلمية

١٩. العتيبي، عبد الرحمن بجاد. (2017) دور الأمن السيبراني في تعزيز الأمن الإنساني، رسالة ماجستير غير منشورة،الرياض، جامعة الأمير نايف العربية للعلوم الأمنية.

٢٠. الشهري، أحمد علي (2019) مقترح للتدابير الوقائية من الجرائم السيبرانية لتعزيز الاعتدال الفكري، رسالة دكتوراه، الرياض، جامعة نايف العربية للعلوم الأمنية.

٢١. العمران، شيخة عمران (2019) العوامل الاجتماعية المرتبطة بالجرائم السيبرانية، رسالة ماجستير، الرياض، جامعة الأمير نايف للعلوم الأمنية.

٢٢. الزهراني، جمعان مبروك (2008) مجالات تطبيق نظم المعلومات في الأجهزة الأمنية وسبل التعامل مع مهدداتها، رسالة ماجستير، جامعة الأمير نايف العربية للعلوم الأمنية

٢٣. الكلالدة، إيمان وأبو راس، أروى (2016) الوعي المعلوماتي وأثره في مجتمع المعلومات، دراسة منشورة في المكتبة الرقمية السعودية، جامعة الأردن.

رابعاً المراجع الأجنبية:

24. Amao (2015) active cyber defense to fight cybercrime ، proquest Dissertations, Detroit, Michigan.
25. Nayak& Yasser (2012) Cybercrime: A threat to network security, internal security journal, Ukraine.
26. Saini Shankar (2012) Cyber-crimes and their impacts ، international journal of engineering research,Washington State University, Pullman.
27. Vasylenko (2012) Problem of cybercrime in Ukraine: spread of specific nature, and methods of fighting, EBSCO, Ipswich, Massachusetts.