مجلة التجارة والتمويل

https://caf.journals.ekb.eg/

كلية التجارة – جامعة طنطا

العدد : الرابع

ديسمبر 2023

(الجزء الاول)

أثر وعى العملاء بالقرصنة الإلكترونية كأداه لتحقيق الأمن السيبراني

" دراسة ميدانية علي البنوك الحكومية بمحافظة بورسعيد "

The impact of customer awareness of electronic piracy as a tool for achieving cyber security

"A field study on government banks in Port Said Governorate"

إعداد

د / شريهان مصطفى التونى

مدرس إدارة الإعمال

المعهد العالي للعلوم الإدارية بالقطامية

dr.sherihan@hims.edu.eg

مستخلص البحث

إن القرصنة الإلكترونية أصبحت من أهم التحديات التي تؤرق الدول والمجتمعات وبصفة خاصة المهتمين بتكنولوجيا المعلومات، لأنها تمس المعلومات التي باتت تمثل أهم العناصر الاستراتيجية في عصر المعلوماتية، **هدف البحث إلى التعرف** على "أثر وعى العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني في البنوك الحكومية بمحافظة بورسعيد مع اختبار العلاقة ميدانيا بين المتغيرين. ومعرفة مدى العلاقة بين أبعاد وعى العملاء بالقرصنة الإلكترونية، الأمن السيبراني من وجهة نظر عملاء البنوك. وبناء على أهداف البحث وتحليل الدراسات السابقة والإطار النظري **تمت صياغة الفرضية الرئيسة** للبحث كالتالي" يوجد تأثير معنوي ذو دلالة إحصائية لوعى العملاء بالقرصنة الإلكترونية بأبعاده الثلاثة (المعرفة، المهارات، الخبرة). على الأمن السيبراني بالأبعاد الثلاثة (الجهود التنظيمية، المتطلبات الفنية، رصد وتقييم التهديدات) "لدى البنوك الحكومية بمحافظة بورسعيد محل البحث . وقد تم تقسيم هذا الفرض الرئيس إلى ثلاثة فروض فرعية لقياس هذه الأبعاد، وقد اعتمدت الباحثة على أسلوب العينة العشوائية من البنوك الحكومية بمحافظة بورسعيد وذلك نظرا لكبر حجم مجتمع البحث فإن أسلوب الحصر الشامل في جميع البيانات الخاصة بالبحث سيكون أمر صعب جدا لاعتبارات الوقت والجهد والتكلفة، وقد استخدامه أداة دراسة متمثلة في "استبانة"، واستند البحث على "المنهج الوصفي"، وتكون **مجتمع البحث** من العملاء بالبنوك الحكومية بمحافظة بورسعيد، وتم توزيع (450) واستخدام برنامج التحليل الإحصائي (SPSS) للإجابة عن أسئلة البحث، وخلصت لمجموعة من النتائج كان أبرزها بأن مستوى ودور إدارة الحماية البنكية كان مرتفعا، وكذلك بينت البحث وجود دور الأمن السيبراني بدلالة أبعاده (الجهود التنظيمية، المتطلبات الفنية، التنسيق مع المؤسسات الأخرى، رصد وتقييم التهديدات) في التوعية والحد من الجرائم المالية، أظهرت نتائج التحليل الإحصائي بأن فاعلية إجراء الرقابة الداخلية في توفير الأمن السيبراني في التصدي للجرائم (القرصنة الإلكترونية) وذلك من خلال توفير آليات مناسبة لتطوير معارف ومهارات للعملاء الحاليين والمستقبليين ورفع مستوى الوعي والإرشاد وتمكينهم من فهم المخاطر الأساسية للمعاملات التي يجرونها مع البنوك والتصدي من عمليات الاحتيال التي يعرض لها العملاء وكيفية توفير وتوضيح الطرق التي من خلالها يقوم المحتالون بخداع ضحاياهم. وبما يمكن العملاء من التصيد لعملية الاحتيالي وقدرتهم علي اتخاذ القرارات المناسبة لهم، وتوجيههم إلى الجهة المناسبة للحصول على المعلومات في حال حاجتهم ولذلك وبناء على نتائج البحث فقد تمت صياغة عدد من التوصيات من أهمها: ضرورة تضافر الجهود بين القطاعات الحكومية ومن ضمنها البنوك في التعاون والتنسيق فيما بينها لأجل تطوير وتحسين

إدارة الأمن السيبراني والقدرة علي توفير الثقافة البنكية ودورها في تحقيق التوعية المصرفية والتصدي للقراصنة الإلكترونية بالاضاقة إلي زيادة الأبحاث المرتبطة بالأمن السيبراني إذ تبين قلة في هذه الدراسات وخصوصا العربية منها.

الكلمات المفتاحية : وعى العملاء – القرصنة الإلكترونية – الأمن السيبراني – القطاع الحكومي

Abstract

Electronic piracy has become one of the most important challenges that worry countries and societies, especially those interested in information technology, because it affects information that has become the most important strategic elements in the information age. The research aimed to identify "the impact of customers' awareness of electronic piracy as a tool to achieve cybersecurity in government banks in Port Said Governorate." By testing the relationship in the field between the two variables, and knowing the extent of the relationship between the dimensions of customers' awareness of electronic piracy and cybersecurity from the point of view of bank customers. Based on the research objectives, analysis of previous studies, and the theoretical framework, the main hypothesis of the research was formulated as follows: "There is a statistically significant effect of customers' awareness of hackers." Electronic technology in its three dimensions (knowledge, skills, experience). "On cybersecurity in the three dimensions (organizational efforts, technical requirements, monitoring and evaluating threats)" among the government banks in the Port Said Governorate under investigation. This main hypothesis was divided into three sub-hypotheses to measure these dimensions, and the researcher relied on the random sampling method from the government banks in the Governorate. Port Said. Due to the large size of the research community, the method of comprehensive inventory of all data for the research would be very difficult due to considerations of time, effort, and cost. A study tool represented by a "questionnaire" was used, and the research was based on the "descriptive approach," and the research community consisted of clients in government banks. In Port Said Governorate, (450) were distributed and the statistical analysis program (SPSS) was used to answer the research questions. It concluded with a set of results, the most prominent of which was that the level and role of the banking protection department was high. The research also showed the presence of the role of cybersecurity in terms of its dimensions (organizational efforts, technical requirements (Coordination with other institutions, monitoring and evaluating threats) in raising awareness and reducing financial crimes. The results of the statistical analysis showed that the

effectiveness of the internal control procedure in providing cybersecurity in confronting crimes (electronic pirates) is through providing appropriate mechanisms to develop knowledge and skills for current and future customers and raise The level of awareness and guidance and enabling them to understand the basic risks of the transactions they conduct with banks, to confront the fraudulent operations to which customers are exposed, and how to provide and explain the methods through which fraudsters deceive their victims. In order to enable customers to detect fraudulent operations and their ability to make appropriate decisions for them, and to direct them to the appropriate party to obtain information in the event of their need, therefore, and based on the results of the research, a number of recommendations have been formulated, the most important of which are: the necessity of concerted efforts between government sectors, including banks, in cooperation and coordination. Among them, in order to develop and improve cybersecurity management and the ability to provide banking culture and its role in achieving banking awareness and confronting electronic pirates, in addition to increasing research related to cybersecurity, as it was found that there is a lack of these studies, especially Arab ones.
Keywords: customer awareness - hackers - cybersecurity - government sector

أولاً : المقدمة

تعد مواكبة التكنولوجيا الحديثة وفهم احتياجات العملاء ووعيهم من أهم التحديات التي تواجهها البنوك، ويتطلب الاعتماد المتزايد على التكنولوجيا في تقديم البنوك لخدماتها المصرفية توافر السرية للمعلومات البنكية عند تنفيذ أي تعامل إلكتروني لتجنب المخاطر (Kalunda,2019) التي يمكن أن تتعرض لها البنوك؛ وفي ظل انتشار فيروس كورونا، تضاعف الإقبال على الخدمات الإلكترونية بشكل غير مسبوق، وخاصة خدمات البنوك، خوفا من العملاء من النزول إلى مقرات البنوك والتعرض للإصابة بالفيروس القاتل، كما تضاعفت معدلات التجارة الإلكترونية بسبب انتشار الفيروس، وزادت أيضا معدلات الجرائم الإلكترونية وخاصة **(Frank,2022)** جرائم النصب على عملاء البنوك، عبر مواقع التسوق الإلكتروني، وشهدت الفترة الأخيرة وقوع العديد من الجرائم ضد عملاء البنوك، من خلال سرقة بياناتهم، والاستيلاء على أموالهم في البنوك، أو شراء بضائع عبر مواقع التسوق بعد سرقة بيانات بطاقاتهم الائتمانية أو البطاقات البنكية.

فيما تسببت الثورة المعلوماتية في ظهور نوعية جديدة من الجرائم المستحدثة والتي تعرف بالقرصنة الإلكترونية أو المعلوماتية والتي تتم عبر وسائل الاتصالات وتكنولوجيا

المعلومات وعبر شبكة الإنترنت، وتتعدد أنماط من هذه الجرائم منها عمليات (Badawy, 2023) النصب وسرقة أرصدة حسابات عملاء البنوك أو اختراق مواقع البنوك والمؤسسات المالية نفسها وسرقتها، مما يكبدها خسائر مادية فادحة، ويسقط الكثير من الضحايا في عمليات النصب الإلكترونية والتي تزايدت في الآونة الأخيرة، لذلك حذر العديد (All elt, 2023) من البنوك وهيئة البريد المصري، عملاءها من الوقوع في فخ عمليات النصب والاحتيال، مطالبة بعدم الإدلاء بأي بيانات عن الحسابات المصرفية حتى لا يتعرضوا للنصب والاحتيال وسرقة حساباتهم.

يعتبر البحث في مجال "وعى العملاء بالقرصنة الإلكترونية"– في واقع الأمر– لا يمكن أن ينحصر تحت مظلة واحدة (Hartmann elt , 2021) ؛ فالباحثون في المجال الأكاديمي يتناولونه باعتباره العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، وكذلك المشتغلون في مجال تقنية المعلومات يتناولونه باعتباره الوسائل والأدوات والإجراءات اللازمة لضمان حماية المعلومات (Kim Lian Lee,2020) من المخاطر، ومن الناحية القانونية عن طريق توفير الثقافة والتوعية اللازمة للعملاء من أجل حمايتهم من الاحتيال والنصب، ويعتبره الدارسون بأنه مجموعة التشريعات والقوانين لحماية المعلومات من الأفعال غير القانونية التي تستهدف تلك المعلومات وأنظمتها (Kamiya elt , 2023).

ومن ثم فإن هذا البحث يستهدف استكشافا "**أثر وعى العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني**" . وتحقيقا لهدف البحث سوف تعتمد الباحثة على المنهج التحليلي لأهم الإصدارات المهنية والدراسات ذات الصلة بموضوع البحث، واختبار فروض البحث من خلال دراسة ميدانية سوف يتم إجراؤها من خلال استمارة استبيان موزعة على مجموعة من الفئات المستهدفة، مع استخدام الأساليب الإحصائية المناسبة.

ثانياً : الدراسات السابقة

بعد مراجعة الباحثة للعديد من الدراسات التي تخص متغيرات البحث الحالي وجدت الباحثة أن هناك مجموعة من الدراسات السابقة التي تناولت العلاقة بين متغيرات البحث ، وفيما يلي عرض للدراسات السابقة التي تناولت العلاقة المباشرة بين وعى العملاء بالقرصنة الإلكترونية والأمن السيبراني ، وذلك على النحو التالي:

أ – عرض وتحليل الدراسات السابقة:

هدفت دراسة (Almatarneh, N. S,2020) إلي قياس ضعف النشاطات التى تعمل على تاخر تثقيف العملاء بالجرائم الالكترونية مما يؤدى إلي عدم قدرتهم على التعامل مع

التقنيات الحديثه لجهلهم وتخوفهم منها كما هدفت الدراسة إلي تحديد آليات تعمل على توعية العملاء وتثقيفهم فى التعامل الإلكترونى وكانت دراسة الحاله على شركة الخدمات المصرفية الإلكترونية حيث جاءت بان اهتمام البنك المركزى بالتقنية المصرفيه أحد برامج اصلاح الجهاز المصرفى بالإضافه إلي اشتراك مجموعة من البنوك التجارية مع شركة الخدمات المصرفية يساعد فى ادخال التقنيات المصرفية والخبرات التقنية أدى إلي تقليل المصروفات الإدارية .اعتمد البحث على المنهج الوصفى التحليلي والاستعانة بالأساليب الإحصائية لتحليل نتائج الدراسة الميدانية .توصلت الدراسة إلي ضرورة الاستمرار فى سياسة الاصلاح المصرفى وتوجيه المصارف فى تفعيل التقنية المصرفية ووضع الخطط المستقبلية ودعم البنية التحتية لمواكبة المنافسة العالمية . **كما كشفت دراسة (على ، 2019)** إلى كيفية التحقيق من العوامل المتعلقة بالتوعية بالأمن السيبراني في القطاع المصرفي البحريني ويركز البحث على دراسة العوامل المرتبطة ب CSA في العمل المصرفي البحريني. تتمثل هذه العوامل في: دعم الإدارة العليا، الميزانية، إنفاذ سياسة الأمن السيبراني، والامتثال للأمن السيبراني وثقافة الأمن السيبراني، واعتمد الباحث على المنهج الوصفي التحليلي، واستخدم الاستبيان كأداة للدراسة ويتكون مجتمع الدراسة من(119) موظف، وتوصلت الدراسة إلى: أهمية دعم الإدارة العليا من أجل الوعي بالأمن السيبراني في البنوك البحرينية ويظهر علاقة كبيرة بين التزام الإدارة العليا والدعم والوعي بالأمن السيبراني وجاء في المرتبة الثانية، أهمية الميزانية للأمن السيبراني في البنوك البحرينية تم الاتفاق عليه بشدة مما يعكس وجود علاقة مهمة بين وضع ميزانية وتخصيص ميزانية ل CSA وجاء في المرتبة الثالثة، أهمية إنفاذ السياسة للتوعية بأمن الفضاء الإلكتروني في البنوك البحرينية التي أشارت إلى أن المشاركين كانوا يعبرون بقوة عن أهمية العلاقة بين تطبيق سياسة الأمن السيبراني ووكالة الفضاء الكندية . **كما هدفت دراسة (محمد،2023)** إلى استنباط فاعلية توظيف العلاقات العامة لتكنولوجيا المعلومات عبر المواقع الإلكترونية في التوعية بالأمن السيبراني: موقع المركز الوطني للاستعداد الطوارئ الحاسبات والشبكات (EG-CERT) نموذجا"، حيث تعد هذه الدراسة من الدراسات الوصفية التحليلية معتمدة في ذلك على منهج المسح الإعلامي باعتباره السب المناهج العلمية ملاءمة للدراسات الوصفية التحليلية ؛ من خلال اعتماد الباحثة على أداة تحليل مضمون المواقع الإلكترونية، بهدف وصف وتحليل مدى توظيف العلاقات العامة لتكنولوجيا المعلومات عبر موقع المركز الوطني للاستعداد الطوارئ الحاسبات والشبكات EG-CERT في التوعية بالأمن السيبراني، ومدى التزامه بمبادئ الاتصال الحواري ونموذجي جودة الويب والجيل الثاني للانترنت في المحتوى النصي لصفحاته وهيئته الشكلية والإخراجية والبرامج والتطبيقات التكنولوجية التي يحتوي عليها. وقد أوصت الدراسة بضرورة

اهتمام الباحثون بإقامة المزيد من الدراسات التي تهتم بدور العلاقات العامة في التوعية بالأمن السيبراني، و العمل على تعزيز التوعية المستدامة بالأمن السيبراني عبر وسائل الإعلام الرقمية من خلال الحملات التوعوية بالإضافة إلى سن قوانين تتعلق بالأمن السيبراني عبر وسائل الإعلام الرقمية وتطوير القوانين الحالية لضبط الأمن السيبراني وحماية فئات المجتمع من أي هجمات وجرائم الكترونية. **يرى (فيصل ، 2023)** ضرورة الكشف عن أثر تدريس مقرر الأمن السيبراني على تنمية الوعي المعلوماتي والمهاري للأمن السيبراني لدى طلاب دبلوم الحاسب في كلية التربية بجامعة حائل، ولتحقيق هذا الهدف، اعتمد الباحث على المنهج شبه التجريبي، وتم بناء مقياس الوعي المعلوماتي والمهاري للأمن السيبراني وبلغ (22) مفردة، وتم التطبيق على عينة من طلاب دبلوم الحاسب البالغ عددهم (45) طالبًا. وقد أسفرت النتائج عن وجود فروق دالة إحصائيا في المقياس ككل عند مستوى (0.5) بين متوسطات درجات طلاب الدبلوم في التطبيق القبلي والبعدي لصالح التطبيق البعدي لمقياس الوعي المعلوماتي والمهاري للأمن السيبراني، مما يدل على وجود أثر لتدريس مقرر الأمن السيبراني على تنمية الوعي المعلوماتي والمهاري، وفي ضوء هذه النتائج، تم تقديم مجموعة من التوصيات والمقترحات. **ومن ناحية أخرى وضح (Aduda, J., Kalunda,2019)** التهديدات التي يواجهها الامن السيبراني داخل المؤسسات المالية ، وقد تكون تهديدات داخلية مثل مبالة الموظفين ، سرقة البيانات التي تتمثل بعمليات القرصنة ، وتطرقت إلى كيفية التعامل مع التهديدات الداخلية والخارجية ، كعمل حملات توعية مستمرة حول أهمية أمن المعلومات في المصارف ، ومصادقة المستخدم والتصريح بالدخول ، وأيضا تناولت الحديث عن المخاطر التي يواجهها كل مصرف أو مؤسسة مالية ، وتوصيات من أجل مصرفية آمنة .اعتمد البحث أسلوب المسح بالنسبة (للزبائن) حيث تم إعداد استمارة تتضمن مجموعة من الأسئلة لاستقراء آرائهم .أما بالنسبة للمصرف فقد تم إجراء مقابلات مع بعض المسؤولين في مصرف حكومي ثم في مصرف أهلي لتقصي آرائهم بشان استراتيجية التسويق لديهم. كما أظهرت النتائج أن 22 % قد تعرضوا للسرقة ، وأن 02.77 % قد تعرضوا للابتزاز و20 % قد تعرضوا للتهديدات ، كما تعرض 05.55 % للتشهير. **كما أوصى (Wafaa,2022)** إلى الكشف عن مستوى الوعي بالأمن السيبراني لدى عملاء البنوك بمدينة جدة، واستخدمت الباحثة المنهج الوصفي ب، وبلغت عينة الدراسة (157) عميل، وكان من أهم نتائج الدراسة وجود ضعف في الوعي بمفاهيم الأمن السيبراني لدى عملاء البنوك . كما أكدت دراسة **(Kim,2020)** إلى التعرف على درجة وعي العملاء بالأمن السيبراني، واستخدمت الباحثة المنهج الوصفي، وبلغت عينة الدراسة (104) عميل بالبنك في مدينة الطائف، وأظهرت نتائج الدراسة ارتفاع وعي العملاء بالأمن السيبراني.**استنتاجاً لما سبق**

اتفقت الباحثة مع دراسة (Almatarneh,2023) أن تهديدات الأمن السيبراني من أهم التهديدات التي تواجه البنوك التجارية ومستقبلها ، حيث أن هجمات القرصنه الإلكترونية تتطور بشكل أسرع من تطور الحلول الأمنية ، الأمر الذي يترتب عليه أن تصبح تلك الإنتهاكات الأمنية تمثل جانباً سلبياً على البنوك التجارية وعملائها ، وتعتبر برامج الأمان المعمول بها مثل برامج مكافحة الفيروسات والبرامج الضارة والجدران النارية غير كافية حتى الآن للحماية من مخاطر تكنولوجيا المعلومات وتوفير ضمانات بشأن الأمن السيبراني من خلال دعم وتعزيز المهارات الرقمية للموارد البشرية العاملة بالبنوك التجارية، وذلك لضمان كفاءة وفعالية التعامل مع المخاطر السيبرانية والحد منها ، من خلال توفير دورات تدريبية ومنح دراسية وورش العمل بما يدعم الإستقرار المالي لتلك المنظمات البنكية .

ب – أوجه الشبه بين الدراسة الحالية والدراسات السابقة:

1- اتفقت الدراسة الحالية مع أغلب الدراسات السابقة في المنهج المستخدم، وهو المنهج الوصفي التحليلي.

2- اتفقت الدراسة الحالية مع الدراسات السابقة في استخدام أداة الاستبانة من أجل جمع المعلومات، إضافة إلى تركيز الدراسات السابقة على الأمن السيبرانى كمتغير تابع.

3- اتفقت الدراسة الحالية مع معظم الدراسات السابقة في تحديد أبعاد المتغير المستقل وعى العملاء بالقرصنة الإلكترونية وهى (المعرفة ، المهارات ، الخبرة ، الثقافة .) .

4- أتفقت الدراسة الحالية مع الدراسات السابقة في تناول أهمية الأمن السيبرانى ومفهومة وأثرة على كفاءة المنظمات البنكية .

5- – أتفقت الدراسة الحالية مع الدراسات السابقة أن البنوك تحتاج إلى مزيد من الإستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبني التحتية السيبرانية وتطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.

ج – الفجوه البحثية للداسات السابقة

لم ترصد الباحثة بحث تناول قياس الدور الذى يلعبة وعى العملاء بالقرصنة الالكترونية كأداه لتحقيق الأمن السيبراني وذلك من خلال تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بقطاع البنوك بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني .

د – أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة:

1 – تختلف الدراسات السابقة عن الدراسة الحالية فيما بينها من حيث الأبعاد والمتغيرات التي تم التركيز عليها من جانب كل دراسة مايجعل الباب مفتوح للأبحاث لسد هذه الثغرة البحثية، والإسهام في إثراء الجانب المعرفي فى موضوع وعى العملاء بالقرصنة الإلكترونية والأمن السيبرانى ، كما أن ذلك التنوع أو الاختلاف يثري المعرفة العلمية في جوانب الموضوع، مما أتاح الفرصة للباحث اختيار أكثر المتغيرات مناسبة لمشكلة البحث .

2 – تناولت الدراسات السابقة مناقشة موضوع تطبيق حماية الأمن السيبرانى وتم ربطها بالأداء الأكاديمي، ولكن الدراسة الحالية ركزت على دراسة أثر تطبيق الأمن السيبرانى على الأداء الوظيفى ، ولا توجد دراسات سابقة ربطت بين المتغير المستقل وعى العملاء بالقرصنة الإلكترونية ، والمتغير التابع الأمن السيبرانى.

د – أوجه الاستفادة من الدراسات السابقة:

1– التعرف على مختلف المنهجيات التي تناولت موضوع البحث والأسس العلمية التي استندت إليها هذه المنهجيات في تطبيق التقنيات البحثية المختلفة.

2– التعرف على الأبعاد المختلفة لمتغيرات الدراسة والتي أجمعت عليها معظم الدراسات السابقة بالإضافة إلى المساهمة في صياغة ، وبناء الاستبانة، ومحاورها، وأبعادها.

ثالثاً : مشكلة البحث

أدى التطور في بيئة الأعمال بشكل سريع إلى إتجاه العديد من المنظمات نحو مواكبة إستخدامات التكنولوجيا الحديثة ، حيث تطبق تقنيات وأدوات تكنولوجية متطورة في مباشرة أعمالها لجعلها أكثر كفاءة ، هذا علاوة على قيام معظم المنظمات الكبرى بتخزين بياناتها الهامة عبر الشبكات الإلكترونية ، وفي ذات الوقت تجبر بيئة الأعمال العالمية المنظمات على الحفاظ على بنية تحتية رقمية آمنة لإجراء معاملاتها التجارية وتسمى هذه البنية التحتية الرقمية العالمية المترابطة بالأمن السيبراني، والذي يشتمل على الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والمعلومات الرقمية **(Frank,2022)**.

وفي هذا السياق تعد تهديدات القرصنة الإلكترونية من أهم التهديدات التي تواجه البنوك التجارية ومستقبلها ، حيث أكدت دراسة كل من **(Fortin,2023)** على أن القرصنة الإلكترونية تتطور بشكل أسرع من تطور الحلول الأمنية ، الأمر الذي يترتب عليه أن تصبح تلك الإنتهاكات الأمنية تمثل جانباً سلبياً على البنوك الحكومية وعملائها ، وتعتبر برامج الأمان المعمول بها مثل برامج مكافحة الفيروسات والبرامج الضارة والجدران النارية غير كافية حتى الآن للحماية من مخاطر تكنولوجيا المعلومات وتوفير ضمانات بشأن الأمن السيبراني ، والجدير

بالذكر أن قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 70%[1] وفق تقديرات البنك الدولي وقد تصل تكلفة الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو 300 إلى 380[2] مليار دولار سنوياً حال إتساع نطاق إنتشارها وفقاً لتقديرات صندوق النقد الدولي الأمر الذي دفع البنوك المركزية العربية إلى تشديد التعليمات الرقابية والتي تلزم البنوك بوضع لائحة من التعليمات لائحة من التعليمات لتأمين التطبيقات الإلكترونية ومن أهمها تثبيت برامج الحماية ضد الإختراق **(صندوق النقد العربي . 2022).**

ومع إستمرار تقنيات المعلومات والاتصالات في الابتكار في إيجاد وتقديم طرق جديدة للوصول إلى العملاء فإن البنوك الحكومية تتعرض في الوقت نفسه لمخاطر جديدة ، حيث أن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية وتقويض الأمن والثقة وتعرض الاستقرار المالي للخطر هذا وقد أكدت دراسة كل من البنك الدولي ، **(Ramirez elt,2022)** على أن نسبة العملاء الذين عانوا من الهجمات السيبرانية خلال عام 2021 على المستوى العالمي نحو 78% بزيادة قدرها حوالي 31% مقارنة بعام 2018[3] وذلك وفقاً للتقرير الصادر عن البنك الدولي في هذا الشأن نتيجة لذلك وإعترافاً بالتهديدات الناجمة عن هجمات القرصنة الإلكترونية ومدى أهمية تعزيز قدرة الأجهزة البنكية على تحمل هذه المخاطر والتحوط منها فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر تلك المخاطر الإلكترونية على البنوك ، في هذا الصدد قامت البنوك المركزية العربية بإصدار التعليمات البنكية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الإلكترونية .

ومما لاشك فيه أن القطاع المصرفى يوجه تهديداً كبيراً من الهجمات الإلكترونية ليس فقط بسبب وجود مبالغ طائلة على المحك وإنما أيضا لأن تعرض هذا القطاع للضرر يشكل نواة أساسية لحدوث اضطرابات على الصعيد الاقتصادى. حيث يطالب المهاجمون ضحاياهم بدفع الأموال فى مقابل فك تشفير ملفاتهم الأسيرة، شهدت زيادة هائلة فى النصف الأول من عام 2022 بنسبة بلغت 1318٪[4]. ويصبح الضحايا أمام خيارين غاية فى الصعوبة فإما دفع الأموال الطائلة، أو الرفض ومحاولة استعادة تلك الملفات عن طريق النسخ الاحتياطية. ويستخدم هؤلاء المجرمون العديد من البرامج الخبيثة والمعقدة لاستهداف بيانات الملكية والعملاء وأموال البنوك والعملاء والأوراق المالية أو حتى عبر اختراق الشبكات الأمنية لتلك المؤسسات

---

[1] - التقرير السنوي للبنك الدولي لعام 2021 .
2 - التقرير السنوى لصندوق النقد الدولى 2023 .
[3] التقرير السنوي للبنك الدولي لعام 2018- 2023
[4] - صنـــدوق النقد العربي : سلسلة " موجزسياسات حول" أمن السيبرانى في القطاع المصرفي"، العدد الرابع ، 08-07- 2022

واستخدامها وسيطا لاختراق حسابات أخرى. ومع تعدد الهجمات الإلكترونية يعتقد البعض أن قراصنة الإنترنت جميعهم سواء، ولكن الحقيقة أنهم منقسمون لثلاث مجموعات لكل منها أهدافها ودوافعها.أول هذه المجموعات هم قراصنة القبعات السوداء، وهم ينشرون البرامج الخبيثة بهدف التدمير وربح المال ونشر الفوضى. أما المجموعة الثانية فتقف على أقصى الطرف الآخر، وهم قراصنة القبعات البيضاء . أما المجموعة الثالثة ويطلق عليها القبعة الرمادية وهم كما يقترح اسمهم يقفون على مسافة واحدة من الطرفين فهم يستغلون الثغرات الأمنية ويقومون بنشر الفوضى ليثبتوا نظريتهم بأن المجتمع الافتراضى غير آمن على الإطلاق.

ولمواجهة هذه التهديدات الخطيرة، ينبغى على البنوك التجارية أولا فهم ودراسة هذه التهديدات، والاعتراف بأن هناك فجوة تقنية تزداد يوميا بين الخبراء الأمنيين التقنيين وهؤلاء القرصنة، وبالتالى تنفيذ برامج تدريبية مستمرة للتوعية الأمنية تمكن المصارف من استباق ومنع الهجمات. وتنفيذ برامج مكثفة لتوعية العملاء حتى لا يقعوا فريسة لعصابات سرقة المعلومات الحساسة. **وإنطلاقاً مما سبق يمكن تحديد المشكلة البحثية لهذا البحث من خلال عرض التساؤلات البحثية التالية :**

1 – ماهي القرصنة الإلكترونية وماهي الدوافع والوسائل المستخدمة في تنفيذ عمليات القرصنة الإلكترونية؟ .

2 – ما هي الآليات المتبعة من قبل الأمن السيبرانى لمكافحة ظاهرة القرصنة الإلكترونية؟ .

3 – إلى أي مدى يمكن الإحاطة بالظاهرة وتوعية العملاء والعمل على مجابهتها والحد من أخطارها في الحد من مخاطر القرصنة الإلكترونية في البنوك الحكومية وتأثير ذلك على دعم الأمن السيبرانى .

ثالثاً : أهمية البحث

تبرز أهمية هذا البحث في كونه محاولة من الباحثة لتسليط الضوء على ظاهرة الإجرام التقني باعتباره ظاهرة مستحدثة لاتزال فى حاجه ماسة إلى مزيد من البحث والبحث خاصة مع ظهور هذه الجرائم بشكل واضح ومنتشر في العديد من المجالات وعلى جميع المستويات والاصعدة يمكن القول إن أهمية البحث تتمثل فيما يلي :

1 – التعرف على ظاهرة القرصنة الإلكترونية كونها من المهددات الناجمة عن استخدام التقنيات الحديثة وتناول البرمجيات والطرق المتبعة في الحد منها .

2 – تأتي أهمية البحث نظراً لأننا أمام مرحلة جديدة في مجال النظم المعلوماتية باعتبارها ظاهرة إنسانية واقتصادية واجتماعية لا يمكن أن تتطور بذاتها، كما تكمن أهمية الدراسة من

خلال إلقاء الضوء على هذا الجانب، ومدى تأثير انتشار ثقافة أمن المعلومات وحماية الأنظمة الإلكترونية لأفراد المجتمع لمواجهة التحديات التي يحملها مستقبل الغد.

3 – رصد الدور الذي يقوم به وسائل الوسائل الاعلامى في نشر توعية باساليب القراصنه الإلكترونية وعلاقتها بإدراك وثقافة العملاء فى ضوء توفير الامن السيبراني لحساباتهم .

4 – يكمن أهمية البحث فى تسليط الضوء على الأمن السيبراني وتأثيره بالجرائم الإلكترونية ، مما يثير بعض النقاط الهامة التى توضح الاستخدام الامثل لما تتيحة التكنولوجية الحديثة على الأمن السيبراني .

5 – رصد درجة مواكبة المواقع الإلكترونية المهتمة بالتوعية بالأمن السيبراني للتطور التكنولوجي، ودرجة استفادتها من تكنولوجيا المعلومات والاتصالات الحديثة للتوعية بالأمن السيبراني.

رابعاً : أهداف البحث

يستهدف البحث إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني ، والذى يلعب دورًا محوريًا في معالجة التحديات المستقبلية نظرًا لاستخدامه كتكنولوجيا لإدارة الشبكات.الامر الذى يساعد على نشر التوعية المصرفية للعملاء كأده لتحسين إدارة استخدام المعدات وصيانتها ، وزيادة الإنتاج المصرفي ، وتوسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة . **وفي ضوء مشكلة البحث وما أجرته الباحثة من مسح للبحوث السابقة وتحليلها يمكن القول إن الأهداف الرئيسية لهذا البحث تتمثل فيما يلي :**

1– التعرف على دور البنوك التجارية في نشر الوعى بالقرصنة الإلكترونية تجاه عملائها من خلال الوصول إلى العملاء وتقديم الاحتياطات الأمنية من أجل تحقيق الأمن السيبراني.

2 – الكشف عن مدى اهتمام المصارف التجارية بممارسة نشر وعى العملاء بالقرصنة ونشر ثقافة الادخار تجاه عملائها.

3 – رفع الوعي لدى العملاء والعاملين في المجال القانوني والأجهزة العاملة على مكافحة تلك الجرائم .

4 – إيجاد حلول لتفعيل التعاون البنكي من أجل وضع اتفاقيات دولية لوضع تشريعات دولية لمكافحة اختراق النظم الإلكترونية ، ووضع معايير لتنظيم استخدام تكنولوجيا المعلومات البنكية سواء على المستوى الفردي أو الدولي أو المؤسسات من أجل التعاون الدولي لمنع وقوع الجرائم وتسليم المجرمين.

5. التعرف على دور الرصد وتقييم التهديدات في التوعية والحد من الجرائم المالية من وجهة نظر العاملين في وحدة تكنولوجيا المعلومات في البنوك التجارية .

6 – الكشف عن مدى وجود فروق ذات دلالة إحصائية في معدلات إجابات عينة البحث حول الأمن السيبراني في التوعية والحد من الجرائم المالية من وجهة نظر عملاء البنوك وتعزى للمتغيرات الوسيطة المتمثلة في (النوع الاجتماعي ، العمر، المؤهل العلمي، والخبرة العملية، الدورات التدريبية).

خامساً : فرضية البحث

للإجابة على التساؤلات السابقة يمكن صياغة الفرضية الرئيسة للبحث كالتالي:

"يوجد تأثير معنوي ذو دلالة إحصائية لوعى العملاء بالقرصنة الإلكترونية حول واقع الأمن السيبراني" محل البحث. ولقد تم تقسيم هذا الفرضية **إلى ثلاث فرضيات فرعية** كما يلي:

H1a–1: يوجد تأثير معنوي إيجابي لوعى العملاء بالقرصنة الإلكترونية على **الجهود التنظيمية** للأمن السيبراني محل البحث.

H1b–2: يوجد تأثير معنوي إيجابي لوعى العملاء بالقرصنة الإلكترونية على **المتطلبات الفنية** للأمن السيبراني محل البحث.

H1c–3: يوجد تأثير معنوي إيجابي لوعى العملاء بالقرصنة الإلكترونية على **رصد وتقييم التهديدات** للأمن السيبراني محل البحث.

سادساً : منهجية البحث

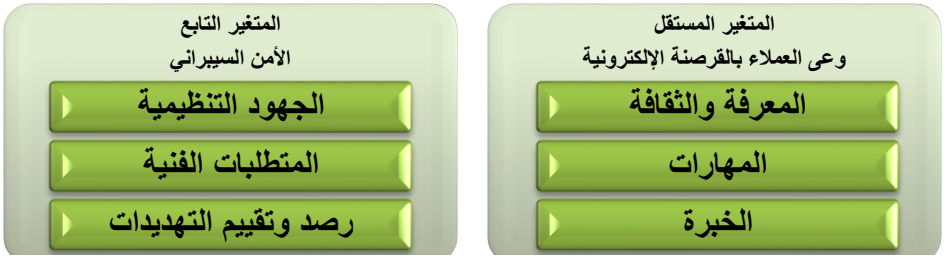
اعتمد البحث على المنهج الوصفي وذلك من خلال الاطلاع المصادر العربية والاجنبية من كتب ودوريات وأبحاث ورسايل جامعية ودراسات ومقالات ، من الانترنت والندوات المنشورة فى الصحف واستباط المتغيرات التى سوف يتم قياسها بأداة الدراسة وهى الاستبانة المستخدمة للقياس وتحليلها للتوصل إلي نتائج منطقية تدعم الفرضيات النظرية الواردة فى الدراسة للتعرف على مدى وعى العملاء بالقرصنة الالكترونية وأثرها على سرية الأمن السيبراني فى القطاع البنكي ، كذلك تم الاعتماد على المنهج الوصفي الذى يحاول من خلاله وصف الظاهرة موضوع البحث ، تحليل بياناتها والعلاقة بين مكوناتها والآراء التى تطرح حولها والعمليات التى تتضمنها والآثار التى تحدثها وكذلك تم الاعتماد علي المنهج التاريخي في استعراض الدراسات السابقة .

مما سبق يمكن استعراض نموذج متغيرات البحث من خلال الشكل رقم (1) والذي يوضح الارتباط والتأثير بين المتغيرات الرئيسية والفرعية. باعتبار متغير وعى العملاء بالقرصنة

الإلكترونية بأبعاده الثلاثة كمتغير مستقل، في حين أن متغير الأمن السيبراني بأبعاده المختلفة يمثل المتغير التابع.

شكل رقم (1)

نموذج متغيرات البحث



المصدر: من إعداد الباحثة بالاعتماد على مراجعة الدراسات السابقة.

سابعاً : حدود البحث

تتمثل حدود البحث فى الحدود الموضوعية والمكانية والزمانية على النحو التالي:

أ – الحدود الموضوعية :

إقتصرت الدراسة على العلاقات بين المتغير المستقل (وعى العملاء بالقرصنة الإلكترونية) ويتضمن الأبعاد التالية (**المعرفة ، المهارات ، الخبرة ، الثقافة**) وبين المتغير التابع (الأمن السيبراني) ويتضمن الأبعاد التالية (**الجهود التنظيمية ،المتطلبات الفنية ، رصد وتقييم التهديدات**)

ب – الحدود المكانية : تتمثل فى البنوك الحكومية بمحافظة بورسعيد.

ج– الحدود الزمنية : تغطى هذه البحث من 2023/7 حتى إنتهاء البحث .

سابعاً : مجتمع وحجم عينة البحث

نظراً لعدم توافر إطار محدد لمفردات مجتمع البحث الذين يتعاملون مع البنوك الحكومية وبالاعتماد على الارقام الواردة من البنك المركزى للتعبئة والاحصاء فإن المجتمع يزيد عن 100000 مفردة ، وعليه يصبح الحد الأدنى لعينة البحث 384 مفردة . وقد اعتمدت الباحثة على اسلوب العينة العشوائية وذلك نظرا لكبر حجم مجتمع البحث فان إسلوب الحصر الشامل فى جميع البيانات الخاصة بالدراسة سيكون أمراً صعباً جداً لاعتبارات الوقت والجهد والتكلفة ، لذلك اعتمدت الباحثة على أخذ عينة عشوائية من البنوك الحكومية بمحافظة بورسعيد وذلك لظروف وإمكانيات الباحثة ، وقد تم تحديد حجم العينة الاجمالية باستخدام المعادلة التالية:

$$\text{ن} = \frac{\text{ق}\,(1-\text{ق})}{\frac{\text{ق}\,(1-\text{ق})}{\text{ن}1} + \frac{\text{د}^2}{(\text{د.م})^2}}$$

حيث :

ن = حجم عينة الدراسة .

ق = نسبة تتراوح بين الصفر والواحد ونفترضتها 05.

ن1 = حجم مجتمع الكلي .

د = نسبة الخطا المسموح بها ونفترضتها 05.

د.م = الدرجة المعيارية وهى تساوى 1.96 عند معامل ثقة 95% .

وبالتعويض فى المعادلة السابقه :

$$ن = \frac{(1.96)^2 (.05) (1 - .05)}{(.05)^2} = 384 \text{ مفردة .}$$

ومن الجدير بالذكر أنه وللتاكد من مصداقية حجم العينة قام الباحث بالرجوع الى الجداول الاحصائية بتحديد حجم العينة (بازرعة ، 1994)[5] وقد وجدت الباحثة أن حجم العينة الناتج من استخدام المعادلة المشار اليها سابقاً يتتطابق مع حجم العينة الناتج من استخدام الجداول الاحصائية .

فى ضؤ ما سبق ورغبة من الباحث فى توسيع عينة الدراسة لتقليل نسبة الخطا فقد: قام بتوزيع عدد كبير من استمارات الاستقصاء يبلغ عددها (450) مفردة وتمكنا من الحصول علـــــــى (411) استمارة صحيحة أى بنسبة استجابة 80 % .

ثامناً: خطة البحث

في هذا السياق، تنقسم هذه الورقة البحثية إلى ستة أجزاء بعد المقدمة والتي شكلت الجزء **الأول**، وتشمل، (مشكلة البحث، أهمية البحث، هدف البحث، فرضية البحث، والمنهج والأساليب المستخدمة، وأجزاء البحث)، يذهب الجزء **الثاني** إلى استعراض الدراسات السابقة المرتبطة بمتغيرات البحث والعلاقة بينهما، ويتم في الجزء **الثالث** تناول (وعى العملاء بالقرصنة الإلكترونية) مع إطاره المفاهيمي وتحليل خصائصه وسياساته وتوضيح أهميته وأهدافه واستعراض أبعاده ومراحله المختلفة، كما يعرض الجزء **الرابع** الاطار النظري (الأمن السيبراني) واستعراض مفهومها والوقوف على أهميتها وأهدافها وتناول ممارساتها المتعددة، أما الجزء **الخامس** فيتم فيه تحليل "أثر وعى العملاء بالقرصنة الإلكترونية كأداه لتحقيق الأمن السيبراني"

[5] Jan, Lynna (2004):"Course Design Elements Most Valued by Adult Learners in Blended Online Education Environments", An American perspective. Educational Media International, 41(4), pp327-337

. وأخيرا تنتهى الورقة البحثية بالجزء **السادس** وبه الخلاصة وأهم الاستنتاجات التي تم التوصل إليها من التحليل السابق، ويتمثل الجزء **السابع** في قائمة المراجع.

تاسعاً : الاطار النظري للبحث

1 – الأمن السيبراني

2 – وعى العملاء بالقرصنة الإلكترونية

1 – الأمن السيبراني

يعد الأمن السيبراني من الأمور التي أصبحت تحتل مكانة لدى الباحثين ، خاصة فيما يتعلق بتحديد مفهوم المصطلح ، وظهرت عدة مفاهيم كلها تدور في حول الأمن السيبراني خاصة في ظل التقدم التكنولوجي الذي يشهد حالة تطور وتقدم مستمر، ومهما تباينت الآراء فيه فإنها تؤدي إلى ضرورة حماية المعلومات بشكل دوري **(عبد الرحمن ،2020)** حتى يمكن الرجوع إلى البيانات المطلوبة بسهولة،وهذه العملية يجب إن تتم على الصعيدين رسمي وشخصي ليتم ضبط عملية أمن المعلومات،من خلال آليات ووسائل كفيلة بمنع اختراقها من قبل أشخاص غير مصرح لهم بالدخول.

أ – مفهوم الأمن السيبراني

هو ممارسة تأمين شبكة الحاسوب من المتطفلين عبر تكنولوجيا البرامج والأجهزة المختلفة، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية **(البكرى ، 2019)**. ويشمل أنواع عدة منها جدار الحماية، وأمان البريد الإلكتروني، وبرامج مكافحة الفيروسات والبرامج الضارة .

ب – عناصر الأمن السيبراني

يتطلب تطبيق الأمن السيبراني وجود العديد من عناصر أساسية ، وفيما يأتي توضيح لهذه العناصر:

– الأشخاص

يمثّل هذا العنصر الأشخاص المعنيين بإدارة شبكة الأمن السيبراني، بحيث يجب أن يتوفر لديهم القدرة على التحقق من التهديدات الإلكترونية **(Kalunda, E,2019)** والدخول غير المصرّح به للأنظمة ومعالجتها، وتأمين الرد السريع للحوادث والهجمات.

– السُلطة

يجب تعيين شخص مسؤول عن تنفيذ عملية الأمن السيبراني، حيث يجب منحه النفوذ اللازم والصلاحيات للقيام بالتغيرات التنظيمية المطلوبة، وتطبيق برنامج الأمن السيبراني بسهولة.

- **الدعم من الإدارة العليا**

يجب الحصول على الدعم والتأييد من مجلس الإدارة، وفريق القيادة، وما يليه في التسلسل الإداري في الشركات، إذ يجب أن يتمتع برنامج الأمن السيبراني بالدعم التام لضمان نجاح تطبيقه.

- **العملية الفعّالة**

يجب أن يشتمل برنامج الأمن السيبراني على نهج فعّال يضمن إدارة عملية الأمن ومواجهة المخاطر الإلكترونية، بحيث يجب أن تحدد عملية الاستجابة للحوادث الإلكترونية الفعّالة كيفية استخدام الأشخاص للأدوات والتقنيات، وكيفية التصدي للهجمات الإلكترونية المُكتشفة.

- **التقنيات المناسبة**

يجب أن تكون التقنيات المُستخدمة في برنامج الأمن السيبراني قادرة على مواجهة 75٪ من التهديدات المُكتشفة، والتحقيق في ما نسبته 25٪ من التهديدات المحتملة، والتي تشكّل خطورة، وبالتالي يجب التحقق من صحتها من قِبل الأشخاص ذوي الخبرة.

- **التواصل في الوقت المناسب**

تضمن عملية التواصل الداخلية في برنامج الأمن السيبراني والتي تحدث في الوقت المناسب لنجاح برنامج الأمن **(سامي ، 2021)** ، إذ يجب التنسيق بين فريق الأمن السيبراني وبين الجهات التي تتطلب الحماية من خلال مسؤولي الشبكات ، ومهندسي الأنظمة .

- **الميزانية**

يتطلب نجاح برنامج الأمن السيبراني على المدى الطويل تخصيص ميزانية مناسبة له، والذي يعد أحد أهم عناصر الأمن السيبراني.

ج – أنواع الأمن السيبراني

يُصنف الأمن السيبراني إلى عدة أنواع، وفيما يأتي أشهرها:

- **أمن الشبكة**

يُعنى أمن الشبكة **(Network Security)** بتوفير الحماية لشبكة الكمبيوتر من تهديدات المتطفلين**(محمد ، 2021)** ، وتكون هذه التهديدات إما من المهاجمين المُستهدفين أو من البرامج الانتهازية الضارّة .

- **أمن التطبيقات**

يهتم أمن التطبيقات **(بالإنجليزية: Application Security)** بإبقاء البرمجيات، والأجهزة دون أي تهديدات، إذ يمكن أن يسهّل التطبيق المُخترق إمكانية الوصول إلى البيانات

التي صُممّت لتأمين الحماية، وبالتالي فإنَّ برنامج الأمن الناجح يبدأ في مرحلة التصميم الأوليّة، أي قبل نشر البرامج أو الأجهزة.

- أمن المعلومات

يركّز أمن المعلومات على تأمين الحماية لسلامة البيانات وخصوصيتها(**عزت ، 2018**) ، وذلك أثناء عملية تخزينها، أو أثناء عملية تناقلها.

- الأمن التشغيلي

يندرج تحت مظلة الأمن **التشغيلي (بالإنجليزية: Operational Security)** العمليات والقرارات المرتبطة بمعالجة أصول البيانات وحمايتها، بالإضافة إلى الأذونات التي يحتاج لها المستخدمين للوصول إلى الشبكة، والإجراءات الخاصة بكيفية ومكان تخزين البيانات أو مشاركتها.

- الاسترداد بعد الكوارث واستمرارية الأعمال

يهتم هذا النوع من الأمن بتحديد الكيفية المتبّعة في استجابة المنظّمة لحادث أمن سيبراني أو أي حدث آخر يؤدي إلى فقدان العمليات أو البيانات.

- تعليم أو تثقيف المستخدم الجديد

يجب الأخذ بعين الاعتبار تعليم الأشخاص، إذ يمكن أن يتسبّب أي شخص دون قصد بإدخال أحد الفيروسات إلى نظام الأمن نتيجة عدم اتبّاع ممارسات الأمن الصحيحة، بحيث تعد عملية تعليم المستخدمين لآلية حذف مرفقات رسائل البريد الإلكتروني المشبوهة، وعدم توصيل محركات الأقراص مجهولة المصدر(USB)، وغيرها من أهم الأمور الواجب تعلّمها. (البكرى ، 2019) .

د - أهمية الأمن السيبراني

تكمن أهميّة الأمن السيبراني في عدة جوانب وفيما يأتي أبرزها:

- يشمل كافة الأمور المرتبطة بحماية البيانات من المهاجمين المُختصين في سرقة المعلومات والتسبب بالضرر، إذ يمكن أن تكون هذه البيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية ، أو بيانات تعريف شخصية ، أو حقوق ملكية فكرية **(Kalunda,2019)**

- يشكّل وجود برامج الأمن السيبراني وآليات الدفاع الإلكترونية وسيلة متطورة ذات أهمية كبيرة في حماية البيانات وخدمة مصلحة الجميع، إذ يعتمد جميع أفراد المجتمع على البُنية التحتية الحيوية كالمستشفيات ، ومؤسسات الرعاية الصحية التي يجب المحافظة عليها.

هـ - نشأة الأمن السيبراني

يُدرج فيما يأتي أبرز المراحل الزمنية التي ساهمت في نشأة الأمن السيبراني:

– تعود نشأة الأمن السيبراني إلى سبعينيات القرن الماضي، بعد أن ابتكر باحث يُدعى بوب توماس برنامجًا على الكمبيوتر يسمّى (Creeper)، حيث ينتقل هذا البرنامج عبر شبكة (ARPANET'S)، تاركًا خلفه مسار تحركاته. **(Abimbola . et al ., 2019)**

– أنشأ مخترع البريد الإلكتروني راي توملينسون برنامجًا يُسمى (Reaper) والذي بدوره قام بحذف برنامج (Creeper)، وبالتالي أصبح برنامج (Reaper) هو أول برنامج لمكافحة الفيروسات.

– ظهرت برامج مضادات الفيروسات **(بالإنجليزية: Antivirus)** التجارية لأول مرة في عام 1987م

– تَوفّر الإنترنت خلال فترة التسعينات، وأصبح متاحًا للجميع، بحيث بدأ الأشخاص بوضع معلوماتهم الشخصية على الإنترنت، حيثُ انتهز مجرمو الإنترنت الفرصة من خلال سرقة البيانات من الأفراد والحكومات عبر شبكة الويب .

– تعد فترة 2000 هي المرحلة التي بدأت فيها المنظمات الإجرامية في تمويل الهجمات الإلكترونية بنحوٍ كبير، وفي المقابل ركزت الحكومات على التشديد في مواجهة جرائم القرصنة.

– تستمر عملية صناعة الأمن السيبراني في النمو والتطور بسرعة كبيرة في عام 2021 م، بحيث يُتوقَّع أن يصل حجم سوق الأمن السيبراني في العالم حوالي 345.3 مليار دولار بحلول عام 2026 م، وذلك حسب إحصائيات شركة (Statista). **(البكرى ، 2019)**

و – متطلبات الأمن السيبرانى :

تتفاوت أهمية المعلومات من حيث مستويات الأمن، ويجب التنويه الى ضرورة وضع نظام حماية يقلل قدر المستطاع من إمكانية كشف المعلومات والتلاعب بها وذلك حسب مستوى أهمية المعلومات ومن ابرز ما هو متعارف عليه الاحتفاظ بنسخ احتياطية ومهما تباينت الآراء وتعددت فأنها في النهاية تدور حول أمن وحماية المعلومات. **(Abimbola . et al,2019)**

س – المعايير المطلوبة للأمن السيبرانى[6]:

استند هذا المعيار إلى وثيقة (ISO) (المعيارية) وهي الوثيقة التي تعنى بتوجيه النصح والإرشاد والتوجيه بهدف إنشاء واستخدام قياسات لأنظمة إدارة أمن وحماية المعلومات

[6] دعت الهيئة الوطنية للأمن السيبراني، اليوم، جميع المهتمين من ذوي المصلحة والمختصين بالأمن السيبراني والعموم إلى إبداء آرائهم ومقترحاتهم حول مسودة وثيقة ضوابط الأمن السيبراني للبيانات .(DCC-1:2021) توضح الوثيقة تفاصيل ضوابط الأمن السيبراني للبيانات، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة، كما أن هذه الوثيقة تعتبر امتدادًا للضوابط الأساسية للأمن السيبراني وتهدف هذه الضوابط إلى توفير الحد الأدنى من متطلبات الأمن السيبراني، لتمكين الجهات من حماية بياناتها خلال دورة حياة البيانات، بالإضافة إلى رفع مستوى الوعي حول التعامل الآمن مع تلك البيانات، وحثت الهيئة على المشاركة وفق النموذج المخصص لذلك عبر الرابط التالي : (https://nca.gov.sa/pages/consultations.html)، ابتداءً من اليوم وحتى الثلاثاء 04/ 04/ 1443هـ، الموافق 09/ 11/ 2021م (ECC - 1: 2018) .ومكملة لها.

مع التركيز على سياسة إدارة نظام امن المعلومات وأهدافه وضوابطه الأمنية التي يتم توظيفها لتطبيق وإدارة الأمن ومنها :

1 – المعلومات الواجب الحفاظ على أمنها وسريتها:

تتفاوت أهمية المعلومات، ودرجة السرية المطلوبة للحفاظ عليها لذلك من الصعب وضع نظام قياسي لتصنيف المعلومات تغطي جميع الإغراض المطلوبة وتكون ملائمة لجميع المواقف كلها، إذ ليس كل المعلومات تتطلب ذات الدرجة **(سناء ، 2019)** من الحماية مثلا المعلومات التي تخضع للشركات الكبرى والمنظمات التي يترصد لها منافسوها للتأثير على سير عمليات الإنتاج هؤلاء يتبعون كافة السبل للوصول إلى المعلومات المهمة لتوظيفها لصالحهم.

- **الأسرار الداخلية للشركات:** وهذا النوع من المعلومات الذي يقع ضمن دائرة السرية المطلقة يجب حمايتها بعناية فائقة،لأنه يكشف مكانة الشركة وأوضاعها المالية.
- **المعلومات المالية:** وهذه المعلومات غالبا ما يهتم بها أصحاب الشركات ورووس الأموال، للتأكد من دقتها وسلامتها، ويتم التحقق منها بشكل دوري لضمان أقصى درجات الحماية لها.
- **معلومات تخص الموارد البشرية:** وهي تلك المعلومات التي تتعلق بالموظفين داخل الشركة أو البنك ، وكل ما يتعلق بهم لحماية ملفاتهم وما يتعلق بها من معلومات شخصية و أمور كالرواتب والتأمين والتقارير الصادرة .
- **المعلومات المؤقتة** : هناك بعض المعلومات مثل المخاطبات أو المذكرات اليومية والإجراءات الروتينية المتبادلة داخل الشركات ، ويجب لفت نظر الموظفين إلى أهمية هذه المعلومات المؤقتة وضرورة حفظ أمنها وسريتها لأنه قد يتطلب طارئ معين الرجوع إليها لتكوين تصور معين حول أمر ما.**(Kalunda,2019)**
- **المعلومات التقنية** : وهي المعلومات الفنية التي يستخدمها الموظفين في الإنتاج وغالبا ما يتم تنفيذها من قبل الموظفين دون توثيق لأنهم يعتبرونها من البديهيات التي لا تستوجب التوثيق.
- **معلومات العملاء:** وهنا يجب التنويه إلى أهمية المعلومات الخاصة بالعملاء وضرورة احتفاظ الشركات والبنوك بمعلومات العميل مهما كانت وبشكل دقيق لان هذه المعلومات قد تكون حساسة مع غياب إدراك البعض لحساسيتها لذا يجب **(سامى ،2021)** الاحتفاظ بسرية معلومات العملاء.

- **المعلومات الأمنية :وهي** المعلومات التي تتعلق بشكل دقيق ومفصل فيما يتعلق بطريقة حماية المعلومات الحساسة للشركات ومنع طرق الوصول إليها دون تخويل مسبق**(على ، 2019)**
- **سلعة المعلومات** : وهذه تتعلق بكل ما يندرج تحت حماية قوانين الملكية الفكرية مثل الكتب والأفلام والإعلانات والبرمجيات. **(Rammal, 2020)**
- **ضمان امن وحماية كلمة السر:** وهذه الوسيلة تعتبر من الوسائل التي يجب أن تضمن الحفاظ على كلمات السر للميولة دون الوصول غير المشروع إليها .

ح – مبادئ الأمن السيبراني

لابد من وجود مبادئ التي يمكن من خلالها ضمان تحقيق أهداف امن وحماية المعلومات خاصة في ظل ما تشهده حركة التقدم التكنولوجي من تسارع كبير [7]ومن أبرزها :

- **الأخلاقيات** : وهي ركيزة مهمة تحرص على التزام البنوك بأخلاقيات التعامل وإدارة العمليات الخاصة بأنظمة المعلومات **(سليمان ، 2020)** .
- **مبدأ المسؤولية** : يجب وضع أطر توضح سياسة الأمن السيبراني ، بحيث تكون المسؤوليات والمهام واضحة إلى جميع الموظفين **(سامى ، 2021).**
- **مبدأ التناسبية** : وهذه من المبادئ التي يجب أن تحقق مستوى من التناسب بين رقابة أمن المعلومات مع أمكانية إجراء تعديلات فيها .
- **مبدأ التكامل:** يجب إن تشكل المعايير والمبادئ والوسائل المتبعة لضمان أمن وحماية المعلومات حلقة متكاملة مع انسجامها مع السياسات والإجراءات المتبعة لحفظ المعلومات بها **(Kim Lian Lee,2020)**

2 – وعى العملاء بالقرصنة الالكترونية

شهد العصر الحالي ثورة معلوماتية كبيرة أثرت بشكل مباشر في حياة الإنسان من حيث الشكل والمضمون، وأدت إلى إيجاد بيئة اجتماعية لم تكن مألوفة من قبل يطلق عليها " البيئة الرقمية، أو الإلكترونية، وكان من نتائجها المباشرة **(Fortin,2023)**أنها أصبحت أداة للكثير من العلاقات والممارسة العديد من الأنشطة ورافق هذا النشاط العديد من الأفعال التي التي شكلت أفعالاً مجرمة بحكم القانون وأبرزت شكلاً من الجريمة أطلق عليها الجريمة

[7]– قامت الباحثة بالاطلاع على ارشادات الهيئة الوطنية للأمن السيبراني في وضع الإرشادات المتعلقة بالمبادى الأمن السيبراني وضمن جهود التعاون والتكامل بين الهيئة ومجلس التجارة الإلكترونية، فقد تم إصدار وثيقتي إرشادات الأمن السيبراني لموفري خدمة التجارة الإلكترونية و إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية.
وتُقدم الوثيقتان إرشادات خاصة بموفري خدمة التجارة الإلكترونية من أصحاب المنشآت الصغيرة والمتوسطة وأصحاب المكاتب الصغيرة والمنزلية لحماية بيانات وأجهزة وخدمات التجارة الإلكترونية الخاصة بهم. كما تُقدم الوثيقتان الإرشادات اللازمة لمستهلكي التجارة الإلكترونية لتحقيق تجربة تسوق إلكترونية آمنة تُساهم في حماية أجهزتهم وحساباتهم ومعلوماتهم الشخصية أثناء عمليات التسوق الإلكترونية.

الإلكترونية"، وشكل هذا النشاط المستحدث العديد من الضحايا حيث أنها توسعت وانتشرت انتشاراً سريعاً في وقت قياسي أصبح مستخدموها من جميع الفئات العمرية بإختلاف مستوياتهم التعليمية.

أ – مفهوم الوعي بالقرصنة الالكترونية

عرف **(على ، 2019)** هو القدرة على صنع قرارات فعالة والإلمام الكافي بالقضايا والتحديات التي تخص إدارة النقد والثروة والتي تجعل القطاع العائلي ذات فعالية أكبر في إتخاذ القرارات المالية.

ب – أهمية الوعي بالقرصنة الالكترونية

تكمن أهمية الوعي بالعمل المصرفي فى النقاط الآتية

1 – قدرة العملاء على فهم آلية العمل المصرفي .

2– التقدم التكنولـــوجي وشبكـــات المعلومات والخـــدمات المصرفية المتعـــددة تتطـــلب الاستيعـــاب لـ (واجب الوقت) أو الإستجابة الصحيحة **(محمد , 2019)** لكيفية التعامل مع هذه الخدمات من قبل العاملين بالمصارف من جهة ، أو من قبل العملاء من جهة أخرى .

3– النقد مظهر من مظاهر استيقاظ الوعي ، وهو الذى يجدد الأبنية الفكرية حين يصقلها ويجعلها فى حالة من التوهج والإشعاع .

ج – معوقات نشر الوعي بالقرصنة الالكترونية:

يواجه نشر وعى العملاء بالقرصنة عدداً كبيراً من المعوقات :

1 – نقص خبرة الموظفين وكفاءتهم وافتقارهم إلى[8] روح المبادرة والاجتهاد ، خوفاً من المساءلة في ظل نظرة الإدارات المصرفية إلى المواطن كصاحب حاجة في تعامله مع المصرف ، وليس كزبون يجب السعي لإرضائه .**(سليمان ، 2020)**

قامت الباحثة بالاطلاع على تقارير البنك المركزى السنوية ولاحظت أن البنوك تواجه القرصنة المصرفية بحلول وتقارير مستمرة حيث حيث اوضح مدير نظم المعلومات ان البنوك لابد أن تعتمد تصميم الموقع الرئيسي الخاص بها من الجهات المعتمدة دوليا بعد انتشار ظاهرة تقليد تصميم مواقع البنوك الرئيسية لايهام العملاء بأن البيانات التي يقوم القرصان بارسالها تتم بالطرق الصحيحة، مشيرا الي ضرورة قيام البنوك بعمليات توعية لعملائها توضح لهم عدم الاستجابة الي أي رسائل تصل إليها من البنك الا بعد مراجعتها مع الادارة والتأكد من صحة البيانات من مركز الكول سنتر. وتعتمد عمليات القرصنة في الغالب علي رسالة توضح رغبة ادارة البنك في تحديث بيانات العميل، وبالتالي يقوم القرصان باستخدام تلك البيانات للقرصنة علي الحساب البنكي.

واعلن مكتب التحقيقات الفيدرالي »إف بي آي« في نهاية العام الماضي عن القبض علي عشرات الاشخاص في مصر والولايات المتحدة بتهمة القرصنة الالكترونية لاستهداف المصارف الامريكية.

8 - وشدد خبراء أمن المعلومات ومسئولو تكنولوجيا المعلومات بالبنوك المصرية علي ضرورة توخي العملاء الحذر في تعاملاتهم مع أي رسائل تصل الي بريدهم الالكتروني تستهدف تحديث بياناتهم، وذلك بعد ما اظهرت تحقيقات النيابة في قضية القرصنة المتهم فيها 43 شابا مصريا غالبيتهم طلبة جامعات باختراق حسابات أموال بنك أوف أمريكااستخدامهم لتطبيقات اصطياد العملاء في ايهام عملاء البنك بتسليم ارقام حساباتهم

2 – غياب الإستثمارات المصرفية المميزة ، إنعكس بشكل سلبي على المواطنين والإدارات المصرفية على حد سواء ما أدخل كلا الطرفين في إرباكات وتعقيدات عديدة ، ودفع المواطن إلى البحث عن منافذ أكثر أمناً لمدخراته .

د – متطلبات وعى العملاء بالقرصنة

1 – الشمولية : الوصول إلى جميع الأفراد لا سيما الأكثر احتياجاً وللأجيال المستقبلية من المستهلكين والمستثمرين . **(Rammal, 2020)**

2 – المشاركة : مساعدة جميع الأفراد على أهمية وعى العملاء بالقرصنة .

3 – التنوع : تقديم التعليم

عاشراً : الأساليب الإحصائية المستخدمة في تحليل البيانات

أ) المجتمع والعينة

يمكن تعريف المجتمع بأنه "مجموعة من المفردات أو العناصر التي يتوافر فيها خصائص ظاهرة معينة" ، ونظراً لصعوبة تجميع البيانات من جميع أفراد المجتمع يمكن اختيار عينة ممثلة له ويتمثل مجتمع البحث في جميع عملاء البنوك الحكومية بمحافظة بورسعيد .

ب) وحدة المعاينة

وحدة المعاينة عبارة عن عنصر واحد من أعضاء العينة ، كما أن العنصر عبارة عن فرد من أفراد المجتمع وبالتالي ، في هذا البحث ، فإن وحدة المعاينة تتمثل في كل عميل يتعامل مع البنوك الحكومية محافظة بورسعيد .

ج) حجم العينة

نظراً لعدم توافر إطار محدد لمفردات مجتمع البحث الذين يتعاملون مع البنوك الحكومية وبالاعتماد على الارقام الواردة من البنك المركزى للتعبئة والاحصاء فإن المجتمع يزيد عن 100000 مفردة ، وعليه يصبح الحد الأدنى لعينة البحث 383[9] مفردة .

د) الأساليب الإحصائية المستخدمة في تحليل البيانات

لقد تم استخدام الحزمة الإحصائية للعلوم الإجتماعية (spss) في تحليل البيانات التي تم جمعها في هذا البحث . وذلك بعد قيام الباحثة بمراجعة الاستبيانات المستردة والتاكد من دقة الاستجابات وصحة الردود، وقد تم استخدام أكثر من أداة إحصائية لتحليل النتائج وذلك لتحقيق أهداف البحث.

---

[9] **تم احتساب حجم العينة وفقا لبرنامج**

https://www.surveysystem.com/sscalc.htm sample size calculator

وفيما يلي توضيح لأهم الادوات الإحصائية التي تم استخدامها:

أ – اختبار كرونباخ ألفا للثبات:

لقد تم الاعتماد على هذه الأداة في التحقق من الاتساق والانسجام الداخلى لأداة القياس للتأكد من ثباتها . فقد قامت الباحثة بحساب معامل كرونباخ ألفا الناتج عن تحليل عناصر الاستقصاء فكلما كانت قيم كرونباخ ألفا عالية كانت درجة الاتساق الداخلى عالية ومقبولة ومؤشراً على ثبات أداة القياس.

ب – الأساليب الإحصائية الوصفية :

تحقيقاً لأهداف هذا البحث وللتعرف على عملاء البنوك نحو تطبيق الشمول المالي قد تم استخدام الأساليب الإحصائية الوصفية والمتمثلة في النسب والمتوسطات الحسابية والانحرافات المعيارية .

ج – التحليل الإستنتاجي لمتغيرات الدراسة

1) تقييم نموذج القياس

هو عملية منظمة مبنية على القياس يتم بواسطتها إصدار الحكم (التقييم) على الشيء المراد تقويمه في ضوء ما يحتويه من الخاصية الخاضعة للقياس ونسبتها إلى قيمة متفق عليها أو معيار معين .

2) النموذج الهيكلي للدراسة

نموذج المعادلة الهيكلية هي مجموعة من التقنيات الإحصائية التي تسمح بفحص مجموعة من العلاقات بين متغير واحد أو أكثر من المتغيرات المستقلة ومتغير واحد أو أكثر.

أولاً : التحليل الوصفي (توزيع عينة البحث وفقاً للخصائص الديموغرافية) :

أ) توصيف عينة الفئة العمرية في البنوك الحكومية

يوضح الجدول التالي توزيع العينة وفقاً لنوع المستقصى منهم من حيث الفئة العمرية في البنوك الحكومية . جدول (1)

الخصائص الديموغرافية لعينة الدراسة (411)

البيان	العدد	النسبة المئوية %	النسبة التراكمية
أقل من 30 سنة	68	16.5	16.5
من 30 إلى أقل من 40 سنة	58	14.1	30.6
من 40 إلى أقل من 50 سنة	225	54.7	85.3
من 50 سنة فأكثر	39	9.5	94.9
بدون بيانات	21	5.1	100
الإجمالي	411	%100	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

نستنتج من الجدول السابق ما يلي :

1) حصلت الفئة العمرية من 40 إلى 50 سنة على النسبة الأكبر والتي بلغت 54.7 % وذلك بعدد مفردات تساوي 225 مفردة وتعتبر هذه الفئة الأكثر دخلا واستقرارا من الناحية المالية.

2) الفئة العمرية السائدة في عينة البحث هي عينة متوسطة العمر، حيث الخبرة والدراسة والدراية بالمشكلات الإدارية والقدرة على حلها لما لديهم من القدرة على مواجهة الصعوبات داخل سوق العمل.

3) ينعكس ذلك بشكل إيجابي على إجابات الاستقصاء لكونها تحتوي على معلومات حديثة نسبياً وما لديهم من معلومات على مدار خبراتهم داخل البيئة البنكية.

4) يوضح ما سبق قدرة المبعوثين بشكل عام على أدارك قضايا الحاسوب وتكنولوجيا المعلومات الخاصة حيث إن جزء منهم يعمل في إدارات الحاسوب.

ب) توصيف عينة للنوع في البنوك الحكومية

يوضح الجدول التالي توزيع العينة وفقاً لنوع المستقصى منهم من حيث النوع في القطاع العام. جدول (2)

الخصائص الديموغرافية لعينة الدراسة (411)

البيان	العدد	النسبة المئوية %	النسبة التراكمية
ذكر	266	64.7	64.7
أنثي	124	30.2	94.9
بدون بيانات	21	5.1	100
الإجمالي	411	%100	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

نستنتج من الجدول السابق ما يلي:

1) أشارت الدراسة إلى أن 65 % من العينة ذكور وهذا يدل على أن الذكور (266 مفرده) أكثر ميلاً من الإناث (124 مفرده) للتعامل مع البنوك .

2) طبيعة العمل الذي يقومون به حيث يتطلب القدرة على التحمل داخل سوق العمل .

3) التأقلم مع المستجدات المحيطة بالعمل في البيئة البنكية .

ج) توصيف عينة المستوى الأجتماعي في البنوك الحكومية

يوضح الجدول التالي توزيع العينة وفقاً للمستوى الأجتماعي لنوع المستقصى منهم من حيث النوع في البنوك الحكومية .

جدول (3)

الخصائص الديموغرافية لعينة الدراسة (411)

البيان	العدد	النسبة المئوية %	النسبة التراكمية
أعزب	61	14.8	14.8
متزوج	297	72.3	87.1
أرمل	16	3.9	91
مطلق	16	3.9	94.9
بدون بيانات	21	5.1	100
الإجمالي	411	%100	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

نستنتج من الجدول السابق ما يلي:

1) بالنسبه للحالة الأجتماعيه ، الفئات الأكثر اهتماماً بالتعاملات البنكيه هم المتزجون بواقع 297 مفردة بنسبة مئوية قدرها 72.3% أما تمثل نسبه فئه الاعزب 14.8% بواقع 61 مفرده

2) يوضح ما سبق قدرة المتزوجين بشكل عام على التفاعل مع النمو المتزايد في الحجم والصعوبات التي تقابلها في المجال المصرفي .

د) توصيف عينة المستوى التعليمى في البنوك الحكومية

يوضح الجدول التالي توزيع العينة وفقاً للمستوى التعليمى لنوع المستقصى منهم من حيث النوع في البنوك الحكومية . **جدول (4)**

الخصائص الديموغرافية لعينة الدراسة (411)

البيان	العدد	النسبة المئوية %	النسبة التراكمية
الثانوية العامة – فأقل	28	6.8	6.8
دبلوم	80	19.5	26.3
بكالوريوس	258	62.8	89.1
دراسات عليا	24	5.8	94.9
بدون بيانات	21	5.1	100
الإجمالي	411	%100	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

نستنتج من الجدول السابق ما يلي :

1) وبالنسبة للمستوي التعليمي، جاءت مفردات العينة الذين حصلوا على (بكالوريوس/ ليسانس) في المركز الأول بواقع 258 مفردة بنسبة مئوية قدرها 62.8 %، يليه في الترتيب الثاني (الدبلوم) بواقع 80 مفردة بنسبة مئوية قدرها 19.5 %، وفي الترتيب الثالث (قبل الجامعي) بواقع 28 مفردة بنسبة مئوية قدرها 6.8 %.

2) يشير ذلك أن النسبة الأكبر من العينة سواءً في البنوك العامة من حملة المؤهلات الجامعية بما يتناسب مع طبيعة عملهم.

3) يشير ما سبق إلى وجود نسبة من الإجابات تعكس بشكل كبير على أهمية المستوى الأكاديمي العالي بما لديهم من درجة علمية كافية لكي يكون مدركاً على معرفة القضايا محل البحث.

4) يتضح أن درجة التعلم التي حصل عليها العملاء لها أَثَرهَا في تنمية معارفهم وتوسيع مداركهم وزيادة ثقافتهم وكذلك الخبرة العلمية والمستجدات التكنولوجيا.

هـ) توصيف عينة نوع الوظيفة في البنوك الحكومية

يوضح الجدول التالي توزيع العينة وفقاً لنوع الوظيفة للمستقصى في البنوك الحكومية .

جدول (5)

الخصائص الديموغرافية لعينة الدراسة (411)

البيان	العدد	النسبة المئوية %	النسبة التراكمية
موظف حكومى	118	28.7	28.7
موظف خاص	169	41.1	69.8
أعمال حره	101	24.6	94.4
عاطل عن العمل	2	.5	94.9
بدون بيانات	21	5.1	100
الإجمالي	411	%100	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

نستنتج من الجدول السابق ما يلي :

1) بالنسبه لنوع الوظيفه ، جاء موظفى القطاع الخاص في المرتبه الاولي بواقع 169 مفردة بنسبة مئوية قدرها 41.1% ، يليه في الترتيب الثاني موظفي القطاع الحكومي بواقع 118 مفردة بنسبة مئوية قدرها 28.7% .

2) تجاوز القيود الهيكلية وذلك لدعم العلاقات لأهداف القدرة التنافسية للحياة العملية .

ثانياً : اختبار صدق وثبات أداة القياس

يوضح الجدول (6) نتائج معاملات الثبات والصدق المتعلقة بعملاء فروع البنوك الحكومية داخل محافظة بورسعيد:

أ – اختبار الثبات والصدق الذاتي لاستجابات عينة بالبنوك الحكومية :

جدول (6)

قيم معاملات ألفا كرونباخ لمقياس وعى العملاء بالقرصنة الإلكترونية فى البنوك الحكومية محل البحث

م	المتغير	عدد الفقرات	معامل ألفا (الثبات)	معامل الصدق الذاتي
1	وعى العملاء بالقرصنة الإلكترونية	10: 1	0.898	0.947

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

أن قيمة معامل ألفا للثبات المتعلقة بوعى العملاء بالقرصنة الإلكترونية (0.898) مما يدل على ارتفاع الثقة والثبات لهذه الاستجابات وإمكانية تعميم نتائجها على مجتمع البحث . وكانت قيمة معامل الصدق للمقياس (0.947) وهو ما يعبر عن صدق العبارات وقدرة المقياس على قياس ما وضع لقياسه .

جدول (7)

قيم معاملات ألفا كرونباخ لمقياس الأمن السيبراني فى البنوك الحكومية محل البحث

م	أبعاد الأمن السيبراني	عدد الفقرات	معامل ألفا (الثبات)	معامل الصدق الذاتي
1	**الجهود التنظيمية**	10: 1	0.957	0.978
2	**المتطلبات الفنية**	10 : 1	0.895	0.946
3	**رصد وتقييم التهديدات**	9 : 1	0.930	0.964

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

يتضح من الجدول رقم (7) أن قيمة معامل ألفا للثبات المتعلقة بأبعاد **الأمن السيبراني** تراوحت بين (0.895) كحد أدني ، و (0.957) كحد أقصى ، مما يدل على ارتفاع الثقة والثبات لهذه الاستجابات وإمكانية تعميم نتائجها على مجتمع البحث . كما تراوحت قيم معاملات الصدق الذاتي لمحاور **الأمن السيبراني** (0.946) كحد أدني ، و(0.978) كحد أقصى وهو ما يعبر عن صدق العبارات وقدرة المقياس على قياس ما وضع لقياسه .

ثالثاً : المتوسطات الحسابية المرجحة والانحرافات المعيارية متغيرات البحث :

تم حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات المستقصي منهم لعملاء البنوك الحكومية محل البحث ، وذلك على النحو التالي :

أ) المحور الأول : وعى العملاء بالقرصنة الإلكترونية (المتغير المستقل) .

جدول (8)

المقاييس الإحصائية الوصفية لبعد " وعى العملاء بالقرصنة الإلكترونية " لفئات عينة البحث

رقم العباره	العباره	المتوسط الحسابي	الانحراف المعيارى	الأهمية النسبية
w1	يهتم البنك بالتواصل مع وسائل الإعلان المحلية لنشر أخباره .	4.7007	.55916	94.014
w2	يتواصل البنك مع العملاء ويبلغهم بكل ما هو جديد.	4.6861	.63344	93.722
w3	يقوم البنك بنشر تقارير مالية لتوعية العملاء مصرفياً	4.7178	.55273	94.356
w4	يتعامل البنك مع معظم الصحف المحلية لنشر إعلاناته باستمرار .	4.5620	.64613	91.24
w5	موظف البنك يقومون بدور أساسي في نشر الوعي المصرفي أثناء وخارج العمل	4.6131	.57060	92.262
w6	يجهز البنك العديد من الملصقات الدعائية لتوعية العملاء من القرصنة .	4.6107	.59615	92.214
w7	لدى البنك موقع انترنت فعال , مصمم بجاذبية ويحدث يومياً بنشر طرق الاحتيال وأساليبها.	4.6472	.52694	92.944
w8	يتواصل البنك مع عملائه من خلال مواقع التواصل الاجتماعي	4.6715	.51480	93.43
w9	تعتبر البنوك المسئولة عن حماية عملاء من الاحتيال المالى	4.6618	.54992	93.236
w10	يدرك المجتمع طبيعة عمل البنك كحلقة وصل بين أصحاب الأموال والباحثين عن تمويل	4.5280	.60973	90.56
الإجمالي	**وعى العملاء بالقرصنة الإلكترونية**	**4.6399**	**0.06109**	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

1) يتضح وجود إختلافات جوهرية بين جميع العملاء في البنوك الحكومية حول " **وعى العملاء بالقرصنة الإلكترونية** " ، كما يدركها فئة العملاء علي حدة فكل منهم تم ترتيب الأهمية النسبية على حسب توقعاته وقدرته على فهم التهديدات الإلكترونية وذلك من خلال وعيهم بالثقافة البنكية.

2) جاءت العبارة الثالثة " **يقوم البنك بنشر تقارير مالية لتوعية العملاء مصرفياً** .في الترتيب الأول للأهمية النسبية (94.356%) وهذا يشير إلىوجود درجة مرتفعة من الموافقة على هذه الفقرة .

3) جاءت العبارة العاشرة " **يدرك المجتمع طبيعة عمل البنك كحلقة وصل بين أصحاب الأموال والباحثين عن تمويل** " . في الترتيب الأخير للأهمية النسبية (90.56%) وهذا يشير إلى وجود درجة منخفضة من الموافقة على هذه الفقرة .

4) ويلاحظ أن المتوسط الحسابي الكلي لإجابات المبحوثين على محور " **وعى العملاء بالقرصنة الإلكترونية** " بلغ (4.6399) ، بانحراف معيارى (0.06109) مما يدل على أن محور " **وعى العملاء** " يحظى بدرجة مرتفعة من الموافقة . **جدول (9)**

المقاييس الإحصائية الوصفية لبعد " الجهود التنظيمية " لفئات عينة البحث

رقم العباره	العباره	المتوسط الحسابي	الانحراف المعيارى	الأهمية النسبية
T1	يتم إعداد وتنفيذ استراتيجية متخصصة للأمن السيبراني	4.6034	.54180	92.068
T2	تستخدم أنظمة الكمبيوتر المتخصصة لتحسين وتطوير الأمن السيبراني	4.7202	.52457	94.404
T3	تتوائم الأجهزة مع مقتضيات ومتطلبات العمل وتطوير الأمن السيبراني.	4.7105	.49026	94.21
T4	يقوم البنك بتحديث أجهزتها بشكل دوري	4.7689	.45543	95.378
T5	يتم تطبيق كل ما هو جديد فيما يخص البرمجيات وبرامج الحماية.	4.8175	.42859	96.35
T6	يقوم البنك بتحديث أجهزتها بشكل دوري لتتوائم مع مقتضيات ومتطلبات الأمن السيبراني .	4.7859	.46632	95.718
T7	يقوم البنك بتوفير ميزانية خاصة التطوير وتحديث الأنظمة الحاسوبية المرتبطة بمنظومن الأمن السيبراني	4.7762	.47217	95.524

T8	يحرص البنك ف علي تقليل المخاطر الائتمانية في ظل التحديات .	4.7786	.47073	95.564
T9	يأخذ البنك آراء العملاء فى أمن المعلومات والمحافظة على مصالحهم	4.7835	.46781	95.67
T10	يعتمد البنك بشكل دائم على مبدأ التحسين المستمر في الخدمات، وقيادة أدائه بالعودة إلى النتائج المحققة وتحليلها ومقارنتها مع النتائج المتوقعة فى ظل التطورات المعاصرة .	4.7056	.59955	94.112
الإجمالي	**الجهود التنظيمية**	**4.7450**	**0.06191**	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

1) إن الوسط الحسابي لإجابات أفراد العينة على العبارات فيما يتعلق بالمحور الأول (الجهود التنظيمية) تراوحت ما بين (4.6034, 4.7835) ويظهر الجدول رقم (9) بأن المتوسط العام لإجابات أفراد العينة حول المحور السابق، بلغ (4.7450) .

2) جاءت العبارة الخامسة " يتم تطبيق كل ما هو جديد فيما يخص البرمجيات وبرامج الحماية." في الترتيب الأول للأهمية النسبية (96.35%) وهذا يشير إلىوجود درجة مرتفعة من الموافقة على هذه الفقرة .

3) جاءت العبارة الأولي " يتم إعداد وتنفيذ استراتيجية متخصصة للأمن السيبراني " . في الترتيب الأخير للأهمية النسبية (92.068%) وهذا يشير إلى وجود درجة منخفضة من الموافقة على هذه الفقرة .

4) ويلاحظ أن المتوسط الحسابي الكلي لإجابات المبحوثين على محور " **الجهود التنظيمية** " بلغ (4.7450) ، بانحراف معيارى (0.06191) مما يدل على أن محور " **الجهود التنظيمية للأمن السيبراني** " يحظى بدرجة مرتفعة من الموافقة.

جدول (10)

المقاييس الإحصائية الوصفية لبعد " المتطلبات الفنية " لفئات عينة البحث

رقم العباره	العباره	المتوسط الحسابي	الانحراف المعيارى	الأهمية النسبية
K1	يقوم البنك بتحسين كفاءة شبكة الحماية بشكل مستمر.	4.5304	.64462	90.608

k2	تتناسب البرامج المتخصصة للحماية مع طبيعة العمل	4.4647	.67397	89.294
k3	الأجهزة المستخدمة تمتاز بمواصفات عالية .	4.5669	.63804	91.338
k4	يتم توفير البرمجيات اللازمة للعمل بشكل دوري	4.4623	.69170	89.246
k5	للحماية البنك قاعدة بيانات احتياطية لجميع المعلومات.	4.4404	.68305	88.808
k6	يقوم البنك بتطوير قاعدة البيانات بشكل دوري ومستمر.	4.4209	.68464	88.418
k7	لدى البنك أنظمة حماية لبياناتها.	4.4404	.69368	88.808
k8	يحرص البنك ف علي تقليل المخاطر الائتمانية في ظل التحديات الالكترونية .	4.3796	.68216	87.592
k9	يحرص البنك في البحث عن العملاء ومخاطبتهم بمختلف شرائح المجتمع .	4.3990	.68887	87.98
k10	يعتمد البنك بشكل دائم على مبدأ التحسين المستمر في الخدمات، وقيادة أدائه بالعودة إلى النتائج المحققة وتحليلها ومقارنتها مع النتائج المتوقعة .	4.4818	.67103	89.636
الإجمالي	**المتطلبات الفنية**	4.4586	0.05711	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

1) إن الوسط الحسابي لإجابات أفراد العينة على العبارات فيما يتعلق بالمحور الأول (**المتطلبات الفنية**) تراوحت ما بين (4.4586, 0.05711) ويظهر الجدول رقم (10) بأن المتوسط العام لإجابات أفراد العينة حول المحور السابق، بلغ (4.7450) .

2) جاءت العبارة الثالثة " الأجهزة المستخدمة تمتاز بمواصفات عالية." في الترتيب الأول للأهمية النسبية (91.338%) وهذا يشير إلىوجود درجة مرتفعة من الموافقة على هذه الفقرة .

3) جاءت العبارة الثامنة" يحرص البنك ف علي تقليل المخاطر الائتمانية في ظل التحديات الالكترونية " . في الترتيب الأخير للأهمية النسبية (87.592%) وهذا يشير إلى وجود درجة منخفضة من الموافقة على هذه الفقرة .

4) ويلاحظ أن المتوسط الحسابي الكلي لإجابات المبحوثين على محور " **المتطلبات الفنية** " بلغ (4.4586) ، بانحراف معيارى (0.05711) مما يدل على أن محور " **المتطلبات الفنية للأمن السيبراني** " يحظى بدرجة مرتفعة من الموافقة . **جدول (11)**

المقاييس الإحصائية الوصفية لبعد " رصد وتقييم التهديدات " لفئات عينة البحث

رقم العباره	العباره	المتوسط الحسابي	الانحراف المعيارى	الأهمية النسبية
P1	البنك متفهم للبنية التحتية المرتبطة بالأمن السيبراني ويتفهم مقدرتها.	4.6350	.61139	92.7
P2	يمتلك البنك شبكة قادرة على حماية عملاء البنوك من المخاطر التي قد يتعرضون لها	4.7080	.56084	94.16
P3	يتم تطوير وتحسين شبكة الحماية بشكل مستمر ودوري	4.7372	.49293	94.744
P4	يقوم البنك بتبني كل ما هو جديد فيما يخص أنظمة الحماية .	4.7397	.47663	94.794
P5	يأخذ البنك بعين الاعتبار الشكاوي من العملاء.	4.7883	.44880	95.76
P6	يستفيد البنك من التغذية الراجعة (Feedback) من ناحية البنك المركزى	4.8686	.39788	97.372
P7	يستفيد البنك من التغذية الراجعة (Feedback)	4.6448	.55466	92.896
P8	يعمل البنك على التزام بالتشريعات القانونية ذات العلاقة للاحتيال البنكي .	4.5815	.58855	91.63
P9	يأخذ بالعبر والدروس فيما يخص نقاط الضعف مع المؤسسات الأخرى.	4.5499	.59208	90.998
الإجمالي	**رصد وتقييم التهديدات**	4.6735	0.11722	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

1) إن الوسط الحسابي لإجابات أفراد العينة على العبارات فيما يتعلق بالمحور الأول (**المتطلبات الفنية**) تراوحت ما بين (4.6735, 0.11722) ويظهر الجدول رقم (11) بأن المتوسط العام لإجابات أفراد العينة حول المحور السابق، بلغ (4.7450) .

2) جاءت العبارة السادسة " يستفيد البنك من التغذية الراجعة (Feedback) من ناحية البنك المركزى." في الترتيب الأول للأهمية النسبية (97.372%) وهذا يشير إلىوجود درجة مرتفعة من الموافقة على هذه الفقرة .

3) جاءت العبارة التاسع " يأخذ بالعبر والدروس فيما يخص نقاط الضعف مع المؤسسات الأخرى.." في الترتيب الأخير للأهمية النسبية (90.998%) . وهذا يشير إلى وجود درجة منخفضة من الموافقة على هذه الفقرة .

4) ويلاحظ أن المتوسط الحسابي الكلي لإجابات المبحوثين على محور " **رصد وتقييم التهديدات** " بلغ (4.6735) ، بانحراف معيارى (0.11722) . مما يدل على أن محور " **رصد وتقييم التهديدات للأمن السيبراني**" يحظى بدرجة مرتفعة من الموافقة .

رابعاً : اختبار فروض البحث

تم اختبار الفروض باستخدام أسلوب تحليل المسار من خلال **برنامج WarpPLS.5** وتم ذلك عن طريق إعداد نموذجين وهما نموذج القياس والنموذج الهيكلي كما يتضح فيما يلي:

أ – تقييم نموذج القياس Measurement model assessment

قامت الباحثة في هذا الجزء باستخدام نموذج المعادلة الهيكلية (Structural Equation Modeling SEM) ، لاختبار الصلاحية وقياس العلاقة بين المتغيرات والتحقق من فروض البحث حيث اعتمدت البحث الحالي على احصائيات نموذج القياس والمتمثلة في :

1) اعتمادية المؤشر باستخدام معاملات التحميل Indicator loadings.

2) اعتمادية الاتساق الداخلي باستخدام الصلاحية المركبة Composite reliability ، وألفا كرونباخ Cronbach's alpha.

3) الصلاحية التقاربية Convergent validity عن طريق حساب متوسط التباين المستخـرج (Average variance extracted(AVE).

4) الصلاحية التمايزية **Discriminant validity** .

جدول (12) صلاحية متغيرات البحث للنموذج أحادي المستوى

العوامل	معاملات التحميل والثبات			الصدق التقاربي	
	كود العبارة	معاملات التحميل	معاملات الثبات	التباين المستخلصِ AVE	الثبات المركب CR
وعى العملاء	w1	(0.739)	.957	.622	.920

بالقرصنة الإلكترونية	w2	(0.797)			
	w3	(0.785)			
	w4	(0.814)			
	w5	(0.830)			
	w6	(0.781)			
	w7	(0.771)			
	w8	--			
	w9	--			
	w10	--			
الجهود التنظيمية	T1	(0.869)	.935	.887	.959
	T2	(0.937)			
	T3	(0.941)			
	T4	(0.929)			
	T5	(0.935)			
	T6	(0.835)			
المتطلبات الفنية	g1	(0.797)	.957	.825	.966
	g2	(0.785)			
	g3	(0.814)			
	g4	(0.830)			

	g5	(0.781)			
	g6	(0.771)			
	g7	(0.759)			
	g8	--			
رصد وتقييم التهديدات	P1	(0.826)	.930	.784	.948
	P2	(0.926)			
	P3	(0.941)			
	P4	(0.935)			
	P5	(0.788)			
	P6				
	P7				
	P8				
	P9				
	P10	(0.826)			

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

ويتضح من الجدول السابق مايلي :

• قامت الباحثة بتقييم اعتمادية (الثبات) العبارات باستخدام التحميلات المجمعة والتحميلات التقاطعية Combined loadings and cross loadings وهذه التحميلات (un– rotated Structure matrix) تحتوي على معامل ارتباط بيرسون بين عبارات القياس والمتغيرات الكامنة، وكانت التحميلات التقاطعية من مصفوفة (rotated Pattern matrix) والتي اشتملت على 34 عبارة والتي تم تحميلها على المتغيرات الكامنة وتراوحت هذه القيم بين(– 1:1).

• جميع المعاملات المعيارية مقبولة. حيث إن قيم المعاملات المعيارية المقبولة لا بد من أن تكون متساوية أو أكبر من 0.50، حيث تم حذف عدد من العبارات (20 عبارة) والتي جاءت نسبتهم أقل من 0.50 حيث تبلغ نسبة معاملات التحميل لكل عبارة تساوي أو أكثر من 0.50، وكانت قيمة المعنوية أقل من 0.05 (P value <0.05)، وتشير هذه النتائج إلى أن عناصر القياس قد استوفت معايير القياس وأن اعتمادية المؤشر قد تحققت.

• تم تقييم الاعتمادية من خلال الاتساق الداخلي والذي يشير إلى مجموعة من العناصر في تقييم البنية الكامنة والتي تحتوي على مجموعة من المؤشرات العاكسة للاعتمادية، ويعد معامل ألفا كرونباخ هو أفضل مقياس يستخدم لتقييم الاعتمادية (Colton & Covert.، 2007)، وكذلك قيمة معامل الثبات المركب (Composite Reliability (CR) حيث يجب أن تكون قيمة معامل الثبات المركب أكبر من (60 %) حتى يكون هناك اتساق داخلي لهذا المقياس، وبالفعل كانت قيمة ألفا كرونباخ والثبات المركب أكبر من (60 %)

• أن قيم الصدق التقارب المعبر عنه بمتوسط التباين المستخلص (AVE) والثبات المركب (CR)، ذات قيم كبيرة، حيث كانت قيم الثبات المركب أكبر من (60 %). قبول الصدق التقارب للنموذج وذلك لارتفاع قيمة متوسط التباين عن 0.5، حيث إن (AVE) المقبولة لابد أن تكون متساوية أو أكبر من 0.5.

• أظهرت نتـائج اختبار الثبات أن جميع معاملات ألفا لكرونباخ مقبولة حيث يرى . (Hair et al.، 2010) أن قيم ألفا المقبولة تتراوح من 0.6 إلى 0.7 في حين أن القيم أكبر من 0.7. تشير إلى درجة عالية من الاعتمادية على المقاييس المستخدمة.

وبناء على ما سبق تم اختبار الصدق التمايزي عن طريق الجذر التربيعي لمتوسط التباين المستخرج ، أو ظهرت نتائج التحليل الإحصائي والتي يوضحها الجدول رقم (12) أن جميع قيم (square root of AVE) مقبولة حيث إن جميع قيم معاملات ارتباط كل بعـــد أو متغير بنفسه أكبر مـــن قيمة ارتبـــاطه ببقية متغيرات البحث الأخـــرى (Hair et al.، 2010)، مما يؤكد وجود صدق تمايزي واتساق عالي للمقياس المستخدم في البحث.

جدول (13)

مصفوفه الارتباط والجذر التربيعي لمتوسط التباين المستخرج Square roots of AVEs

الأبعاد	وعى العملاء بالقرصنة الإلكترونية	الجهود التنظيمية	المتطلبات الفنية	رصد وتقييم التهديدات
وعى العملاء بالقرصنة الإلكترونية	**(0.788)**	0.247	−0.003	0.328
الجهود التنظيمية	0.247	**(0.909)**	0.055	0.098
المتطلبات الفنية	−0.003	0.055	**(0.759)**	0.017
رصد وتقييم التهديدات	0.328	0.098	0.017	**(0.886)**

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى warpls5 .

تشير الصلاحية التمييزية إلى الدرجة التي يختلف بها كل بناء عن التصميمات الأخرى حيث إن البناء يعد متميزاً إذا كانت الصلاحية لتمايزيه مرتفعة، حيث يمكن استخدام الجذر التربيعي لمتوسط التباين المستخرج AVE 's square root لمعرفة الصلاحية التمييزية ويوضح جدول (35) أن الجذر التربيعي لمتوسط التباين المستخرج أكبر من الارتباطات بين التركيبات والتي تحققت لجميع التركيبات، كما عبرت عن وجود ارتباطات معنوية (P <0.001) بين تلك المتغيرات من خلال مصفوفة الارتباط. ثم بعد التحقق من صحة نموذج القياس، ستقوم الباحثة بالانتقال إلى الخطوة التالية وهي تقييم النموذج الهيكلي strctural model assessment.

خامساً : تقييم النموذج الهيكلي strctural model assessment

يمكن وصف النموذج الهيكلي بأنه عبارة عن العلاقات السببية بين المتغيرات الكامنة ، ويهدف إلى اختبار فروض البحث.

جدول (14)

ملائمة النموذج ومؤشرات الجودة Model fit and quality indices

مقياس الملائمة	القيمة الفعلية	قيمة المعنوية values p	الملائمة المقبولة Accepted fit
معامل المسار المتوسط (APC)	0.555	0.001	قيمة المعنوية < 0,05

معامل التحديد المتوسط (ARS)	0.640	0.001	قيمة المعنوية < 0,05
معامل التحديد المعدل المتوسط)(AARS)	0.639	0.001	قيمة المعنوية < 0,05
معامل (AVIF)	1.753	مقبول إذا كان ≥ 5 ، ومثالي إذا كان ≥ 3,3	
GOF	0.554	تزداد جوده النموذج كلما كانت القيمه اكبر من 0.36	
نسبة مساهمة معامل التحديد (RSCR)	1	مقبول إذا كان ≥0,9 ، ومثالي إذا كان=1	

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

وفيما يتعلق باختبارات فروض البحث وفقا للنتائج الإحصائية وذلك في ضوء نتائج النموذج الهيكلي ، يمكن توضيحها في جدول (14) للتأثيرات المباشرة وجـــــدول (15) للتأثيرات غــير مباشرة كما يلي :

سادساً : نتائج اختبارات التأثيرات المباشرة جدول (15)

نتائج اختبارات التأثيرات المباشرة بين المتغيرات

الفروض	الفرض الرئيسي	الفرض الفرعى	اتجاه الفرض	معامل المسار	قيمة معنوية	حجم التاثير	النتيجة
الفرض الرئيسي	**وعي العملاء بالقرصنة الإلكترونية**	←	الأمن السيبراني	0.837	>0.001	0.538	**قبول الفرض الرئيسي**
الفرض الأول	**وعي العملاء بالقرصنة الإلكترونية**	←	الجهود التنظيمية	0.093	0.028	0.834	**قبول الفرض الأول**

الفرض الثانى	**وعي العملاء بالقرصنة الإلكترونية**	←	المتطلبات الفنية	0.153	0.001	0.022	**قبول الفرض الثانى**
الفرض الثالث	**وعي العملاء بالقرصنة الإلكترونية**	←	رصد وتقييم التهديدات	0.156	0.001	0.054	**قبول الفرض الثالث**

المصدر : من إعداد الباحثة وفقاً لنتائج التحليل الإحصائى .

سابعاً : نتائج الفروض

في ضوء مشكلة البحث وأهميته وأهدافه وإعداد الدراسة الميدانية يمكن عرض النتائج التالية:

أ- النتائج النظرية :

1 – تعد الطبيعة المتطورة للقرصنة الإلكترونية غير قابلة للتنظيم بشكل محدد ، كما أن القضايا الخاصة بها يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات

2 – التطور الحادث لدى القرصنة الإلكترونية يحفز المنظمات المالية وخاصة البنوك التجارية على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية ضد تلك المخاطر ، من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك ، الأمر الذي يؤدي إلى دعم الإستقرار المالي في تلك البنوك .

3- تحتاج المراجعة الداخلية في معظم البنوك التجارية الي توسيع قاعدة مهاراتها و اجتذاب مهارات فنية مؤهلة بكافة وسائل التعامل مع تقنيات التكنولوجيا

ب- النتائج العملية :

الفرض الرئيسى : يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني . يتضح من نتائج اختبار الفرض الرئيسى H2 انه بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني . حيث بلغ قيمة معامل المسار (0.837) وكذلك بلــغ حجم التأثير المباشر (0.538) ، وذلك عند مستوى معنــوية (0.001) . وعليه يتضح من النتائج السابقة قبول الفرض الرئيسي الثاني بوجود تأثير معنوي إيجابي مباشر .

1) الفرض الفرعي الأول H2a : يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني (الجهود التنظيمية) .

وفقاً لنتائج التحليل الإحصائي إيجابي بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني (الجهود التنظيمية) . حيث بلغ قيمة معامل المسار (0.093) وكذلك بلغ حجم التأثير المباشر (0.834) ، وذلك عند مستوى معنوية (0.001) . وعليه يتضح من النتائج السابقة قبول الفرض الفرعي الأول بوجود تأثير معنوي إيجابي مباشر .

2) الفرض الفرعي الثانى H2b : يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني (المتطلبات الفنية) .

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية بعد الأمن السيبراني (المتطلبات الفنية) . حيث بلغ قيمة معامل المسار (0.153) وكذلك بلغ حجم التأثير المباشر(0.022) ، وذلك عند مستوى معنوية (0.001) . وعليه يتضح من النتائج السابقة قبول الفرض الفرعي الثاني بوجود تأثير معنوي إيجابي مباشر.

3) الفرض الفرعي الثالث H2c : يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية على بعد الأمن السيبراني (رصد وتقييم التهديدات) .

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي بوعى العملاء بالقرصنة الإلكترونية علي بعد الأمن السيبراني (رصد وتقييم التهديدات) . حيث بلغ قيمة معامل المسار (0.156) وكـــــذلك بلغ حجم التأثير المبـــاشر (0.054) ، وذلك عند مستوى معنوية (0.001) . وعليه يتضح من النتائج السابقة قبول الفرض الفرعي الثالث بوجود تأثير معنوي إيجابي مباشر.

ثامناً : توصيات البحث :

بناء على نتائج البحث ، نقدم التوصيات التالية:

1. تطوير البنية التحتية التنظيمية والتشغيلية والإدارية اللازمة لأجل الارتقاء بإدارة الأمن السيبراني، لما لها دور كبير وأساسي في الحد من الجرائم وبالأخص المالية.
2. ضرورة تضافر الجهود ما بين القطاعات الحكومية والخاصة ومن ضمنها البنوك الحكومية في التعاون والتنسيق فيما بينها لأجل تطوير وتحسين إدارة الأمن السيبراني.
3. ضرورة استخدام الأمن السيبراني كإستراتيجية رئيسية وأساسية لأجل الحد من الجرائم المالية.
4. والتسلسل في ضرورة استخدام البرمجيات الحديثة والتي تهدف إلى كشف الاختراق البنوك الحكومية، لأجل الحد من الجرائم المالية.

5. العمل على زيادة الوعي المصرفي الخاص بجودة الخدمة للموظفين في البنوك، كذلك زيادة اطلاعهم على آخر مستجدات الصناعة المصرفية وطرق الاحتيال المصرفي .

6. تطوير أجهزة الحواسيب وتحميل البرمجيات ذات المواصفات المرتفعة للعاملين في إدارة الأمن السيبراني، بات من الضرورات الملحة بما يتواءم مع متطلبات إدارة الأمن السيبراني، لما لها دور كبير في الحد من الجرائم المالية.

7. يجب على البنوك الحكومية الاستفادة من التغذية الراجعة الناتجة من البنوك الأخرى والتعلم من تجاربها فيما يتعلق بتطوير إدارة الأمن السيبراني لتلافي المشاكل المستقبلية .

8. اتخاذ إجراءات جدية لمواجهة الفساد المالي والإداري، وتمكين الأجهزة الرقابية من ممارسة دورها الرقابي، والعمل على تطبيق اللامركزية الإدارية.

الثاني عشر : المراجع العلمية

أ – الرسائل العلمية

- البسام، سارة عبد الرحمن (2020) ، "**التحقيق في العوامل المتعلقة بالتوعية بالأمن السيبراني في القطاع المصرفي البحريني** "، رسالة ماجستير غير منشورة، البحرين: جامعة الخليج العربي ، ص 129.
- العتيبي، عبد الرحمن بن بجاد ، (2020) ، " **دور الأمن السيبراني في تعزيز الأمن الإنساني**" ، رسالة ماجستير منشورة، السعودية: جامعة نايف العربية للعلوم الأمنية.
- مشتهى ، وصبرى حمدان ، (2022) ، "**مدى موثوقية نظم المعلومات البنكية وأثرها في تحسين مؤشرات الأداء المصرفي**" دراسة مقارنة علي المصارف الأردنية والفلسطينية المدرجة ببيروت عمان ونابلس"، دراسات العلوم الإدارية ، ص 258 .
- خليل ، تيسير ، (2022) ، " **أثر الاستثمار في الأمن السيبراني علي الإداء المصرفي** " ، رسالة ماجستير ، كلية تجارة ، جامعة عين شمس ، ص 86 .

ب – الدوريات العلمية

- محمود عزت ، (2018) ، " **الفضاء السيبراني وتحديات الأمن المعلوماتي العربي**" ، المجلة العربية العدد 49 ، أبريل ، ص 259 .
- حامد هارون على ، (2019) ، " **دور العلاقات العامة في نشر الوعي المصرفي** فى القطاع المصرفي بالبحرين " ، المجلة ادارة الاعمال، جامعة عين شمس ، مجلد 3 ، ص 181– 199 .

- عصام المحاويلي البكرى ، (2019) ، " **تطوير وتنشيط العمل المصرفي ودوره فى تحقيق الوعى المصرفى بالاحتيال البنكي** " ، المجلة العلمية للاقتصاد والتجارة- جامعة عين شمس, العدد الرابع ، 23 – 40 .
- الصحفي، وعسكول، أحمد ، سناء (2019) ، " **مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة**" ، مجلة البحث العلمي في التربية، 20(10)، 493–534 .
- زكريا محمد , (2022) ، " **دور المعهد المصرفي في نشر الثقافة المالية كمحور أساسى فى منظمة البنوك التجارية** " ، الإكاديمية العربية للعلوم الإدارية والمصرفية , المجلد 19 – العدد الأول – السنة 19, يناير 2019 .
- ناصر سليمان ، (2020) ، " **مدى مساهمة البنوك التجارية في نشر الوعي المصرفي لدى العملاء**" ، المجلة العلمية للاقتصاد والتجارة ، كلية التجارة ، جامعة القاهرة ، العدد الأول ، 44 – 66 .
- الوكيل، سامي (2021)، " **الأمن السيبراني.. حماية وطنية لأمن الفرد والمجتمع في المملكة** " ، وكالة الأنباء السعودية، مجلد البحوث العلمية ، ص 152 – 160 .
- عسيري، فيصل محمد ،(2021) " **الأمن السيبراني وحماية أمن المعلومات** "، مجلة الدراسات المالية والمصرفية ،_ كلية تجارة_ ، جامعة أسيوط ، 78 .
- **محمد صابر ، (2023)** " **فاعلية توظيف العلاقات العامة لتكنولوجيا المعلومات عبر المواقع الإلكترونية في التوعية بالأمن السيبراني**" ، المجلة العربية للبحوث الأعلام والاتصال ، جامعة الأهرام الكندية ، مصر ، المجلد2 ، العدد 33 ، ص 15–33 .
- **فيصل بن مهد ، (2023)** ، " **أثر تدريس مقرر الأمن السيبراني على تنمية الوعي المعلوماتي والمهاري للأمن السيبراني لدى طلاب دبلوم الحاسب في كلية التربية بجامعة حائل** " ، العلوم التربوية،العدد الأول .

ج – المراجع الأجنبية

1 – الدوريات الأجنبية

- Aduda, J., Kalunda, E. (2019)," **The dangers of electronic (cyber) attacks and their economic impacts"** Journal of Applied Finance & Banking, Vol. 2, No.6 .pp 142 .

- Akeem , Abimbola . et al . (2019), **"Electronic trapping: methods and countermeasures"** International Journal of Scientific Research and Management (IJSRM), Volume 06, Issue 06.pp37.

- Almatarneh, N. S. (2023)," **Customer awareness of bank fraud",** International journal of economics and finance, 2 (1), 62-69.

- F . G. Rammal, (2020) ." **Awareness of Commercial Banking products among Customers: The case of Australia",** International journal of economics and finance.pp147.

- Badawy, H., (2023) , "**The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions** ": An Experimental Study, Alexandria Journal of Accounting Research, 3 (5) Pp. 1-56

- Frank, M., Grenier, J. and Pyzoha, J., (2022) , **" How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance"**, Journal of Information Systems, 33 (3) , Pp. 183-200

- Hartmann C.C. and J. Carmenate, (2021) , **"Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research, American Accounting Association**, 15 (2) Pp. 9 - 23

- JI O and All, (2023) , **"Evaluation of financial soundness of selected commercial banks in Nigeria An application of Bankometer S-score model** 2 (4) Journal – finance-marketing 2 (4) Pp. 22 – 25.

- Kamiya, S., Kang, J., Kim, J., **and Stulz, R., (2023), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms "**, Journal of Financial Economics, Pp. 719–749

- Fortin, Anne and Heroux, S., (2023), **"Cybersecurity disclosure by the companies on the SPP/TSX60"**, index, vol:19, issue:2, June, pp:73-102

- Ramirez, M, Ariza, L., and Miranda, M.,(2022), **"The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index**), journal of sustainability , 14(3) "

- Sayegh, Wafaa. (2022). **" Customers' awareness of the concept of cybersecurity and its relationship to their security precautions against cybercrimes",** Arab Journal of Social Sciences, 14(3), 18-70

2 - الرسائل الأجنبية –

- Kim Lian Lee, (2020) , **" The role of banks in achieving banking awareness and financial"** , msc , the United States. Environment and planning a Internet Banking and Commerce, 36(2), 251-269. , 36(2), 251-269.