Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (1): 79-94
Doi: www.doi.org/10.25130/tjaes.22.SP7.1.5

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية

EISSN: 3006-9149
PISSN: 1813-1719

The impact of customer perception of digital penetration as a means of achieving cybersecurity: A field study at Rafidain Bank

Shireen Ismail Khalil AL Hadiddy*, Sabah Sabir Mohmad AL Doare, Mohammed Hameed Nayyef
College of Administration and Economics/Tikrit University

Keywords:
Customer perception, Digital penetration, Cybersecurity. Hackers Rafidain Bank.

Article history:

Received	10 Sep. 2025
Received in revised form	16 Sep. 2025
Accepted	2 Dec. 2025
Available online	14 Jun. 2026

*Corresponding author:
Shireen Ismail Khalil AL Hadiddy
College of Administration and Economics/Tikrit University

Abstract: The research aims to determine the extent of customers' awareness of digital penetration and cybersecurity from the perspective of nationalized banks. This research focuses mainly on the impact of customer awareness of digital penetration as a means of achieving cybersecurity. It also highlights the likelihood of users falling victim to digital hacking attacks used to steal banking and personal data. The researcher used the descriptive approach with its theoretical framework, and a questionnaire form to analyze the statistical relationship of a random sample of (50) individuals. (40) valid questionnaires were retrieved for analysis using the statistical analysis program (SPSS) to answer the study questions.

The researcher reached an important conclusion: Cybersecurity and infrastructure security can only be achieved by sensing the methods and practices of attackers and building a strong and secure defense for the "Know Your Customer" (KYC) process for bank customers. This research also seeks to understand the various factors responsible for banking fraud that customers are unaware of**.** In addition to the existence of a statistically significant relationship between the study variables, the increase in the number of digital transactions has paved the way for an increase in fraud and digital hacking. In the current context, cybersecurity and protecting customer information have become one of the greatest challenges. Hackers and cybercriminals have become commonplace and can easily access information anywhere, anytime. Often, customers fall prey to them, unknowingly believing that the mechanism is real, as the researcher's most important recommendation.

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (1): 79-94
Doi: www.doi.org/10.25130/tjaes.22.SP7.1.5

أثر إدراك الزبون بالاختراق الرقمي كَوسيلة لتحقيق الأمن السيبراني: دراسة ميدانية في مصرف الرافدين

شيرين إسماعيل خليل الحديدي صباح صابر محمود الدوري محمد حميد نايف
كلية الإدارة والاقتصاد/جامعة تكريت

المستخلص

يَهدف البحث إلى مَعرفة مدى إدراك الزبائن بالاختراق الرقمي والأمن السيبراني من منظور المصارف المؤممة، كما ويسعى هذا البحث إلى فهم العوامل المختلفة المسؤولة عن الاحتيال المصرفي التي يجهلها الزبون، فضلاً عَن وجود علاقة ذات دلالة إحصائية بينَ مُتغيرات الدارسة، ومهدت الزيادة في عدد المعاملات الرقمية الطريق لزيادة عمليات الاحتيال والاختراق الرقمي. وفي الوضع الحالي، أصبح الأمن السيبراني وحماية معلومات الزبائن من أعظم التحديات. فقد أصبح المتسللون ومهاجمو الشبكة العنكبوتية أمرًا شائعًا، ويستطيعون الوصول بسهولة إلى المعلومات في كل مكان وزمان. وفي كثير من الأحيان، يقع الزبائن فريسة لهم، معتقدين دون علمهم أن الآلية فعلية كأهم توصية للباحثين.

ويركز هذا البحث بشكل رئيس على أثر إدراك الزبون بالاختراق الرقمي كوسيلة لتحقيق الأمن السيبراني؟ وتسلط الضوء على احتمالات وقوع المستخدمين هدفًا لهجمات الاختراق الرقمي والتي تُستخدم لسرقة البيانات المصرفية والشخصية. استخدمت الباحثة المنهج الوصفي بإطارها النظري، واستمارة الاستبانة لتحليل العلاقة الإحصائية لعينة عشوائية تضمنت (50) فرداً تَمَ استرجاع (40) استبانة صالحة للتحليل باستخدام برنامج التَّحليل الاحصائي (SPSS) للإجابة عِن أسئلة الدِراسة، وتوصَلت الباحثة إلى نتيجة مهمة لا يمكن تحقيق الأمن السيبراني وأمن البنية التحتية إلا من خلال استشعار أساليب وممارسات المهاجمين وبناء دفاع قوي وأمن على عملية "اعرف زبائنك " (KYC) لزبائن المصرف.

الكلمات المفتاحية: إدراك الزبون، الاختراق الرقمي، الامن السيبراني، الهاكرز، مصرف الرافدين.

المقدمة

يعد الإنترنت من أهم اختراعات القرن الحادي والعشرين التي أثّرت على حياتنا. لقد تجاوز الإنترنت اليوم كل الحواجز، فأصبح الفضاء الرقمي المصطلح المُفضّل للإشارة إلى العالم الافتراضي الذي تُنشئه أنظمة الحاسوب الشبكية التي تؤثر على أجزاء كبيرة من حياتنا؛ ويُعدّ تأمينه أمرًا صعبًا، فأن "التعقيد عدو الأمن" لا يقتصر الأمر على تزايد عدد الأجهزة المتصلة بالشبكة العنكبوتية، بل يشمل أيضًا تزايد عدد المُصنّعين الذين يُصنّعونها، مما يزيد من حجم وتنوع الأنظمة التي تُشكّل الفضاء الرقمي، وبالتالي من احتمالية الأعطال. علاوة على ذلك، توجَت التهديدات السيبرانية كأبرز التحديات التي تواجه العالم في العصر الحالي، فأصبحت الأنظمة الرقمية المكون الأساسي للبنية التحتية الاقتصادية (Hartman, et al., 2021)، أما في العراق فقَد اكتسب الاقتصاد الرقمي تزايُد الأهمية في تطوير ودعَم القطاعات المختلفة كالتجارة الالكترونية والعمليات المصرفية الرقمية، وعلى الرغم مِنَ ذَلكَ واجهت الدولة تهديدات سيبرانية متصاعدة تستهدف اختراق وسرقة البيانات خاصةَ مَعلومات الأنظمة المصرفية.

يخضع الأمن السيبراني لتفاوتات كبيرة. يُمكن للمهاجمين الاختيار من بين مجموعة كبيرة ومتنوعة من الأساليب، بينما يتعين على المدافعين الانتباه إلى كل التفاصيل والاستعداد لأي شيء في أي وقت مِنَ خلال ادراكهم وزيادة ثقافتهُم الرقمية بهذهِ الهجمة الشرسة. لذلك، لا تُعزى الهجمات السيبرانية الناجحة بالضرورة إلى الإهمال. في بعض الأحيان، تكون ضوابط الأمن موجودة، ولكنها لا تُستخدم بشكل صحيح. فأصبحت أخطار التهديدات السيبرانية أكثر شيوعًا الآن بعد أن أصبحنا نعتمد بشكل شبه كامل على تقنيات الشبكة العنكبوتية (Frank. 2022). بناءً على ذَلكَ حاولت الباحثة جاهدة الوصول إلى هدف البحث مَعرفَة The impact of customer perception of digital penetration as a means of achieving cybersecurity: A field study at Rafid in Bank)، ولِغرض تحقيق هذا الهدف اعتمدت الباحثة على المنهَج التحليلي من خلال سَرد الجانب النظري، واختبار فرضيات الدِراسة معتمدة على دراسة ميدانية تَمَ أجراؤها في مصرف الرافدين فرع تكريت باستخدام استمارة الاستبانة وزعَت على العينة المُستهدفة (الزبائن)، فضلاً عِن استخدام الأساليب الإحصائية.

المبحث الأول: منهجية البحث

أولاً. مشكلَة البحث: أدت التطورات السريعة والمستدامة في بيئة الاعمال توجَه المؤسسات المالية والمصرفية إلى استخدام التقانة المستحدثة وتطبيقها في اعمالها اليومية لجعلها أكثر فاعلية; فضلاً عَن قيام المؤسسات الكُبرى بِتخزين البيانات الحساسة في الحوسبة السحابية، وفي الوقَت ذَاتهِ أجبرت بيئة الاعمال الدولية المؤسسات المصرفية الحفاظ على البنية التحتية الرقمية الآمنة لِغرض اجراء المعاملات المالية والمصرفية في الميدان المبحوث (Frank, et al, 2022: 185)، والتي تكون مرتبطة بالأمن السيبراني، والذي يتضمَن على أنظمة الحاسوب، والانترنيت، والبرمجيات، وامواج المعلومات، والأجهزة، وفي السياق ذاته فأن التهديدات السيبرانية المتمثلة بالاختراق الرقمي تعَد مِن أهم التهديدات السيبرانية التي تواجه حاضر ومستقبل المصارف المالية (Fortin & S, 2023: 75).

بناءً على ذَلكَ يَنبغي على المؤسسات لمواجهَه هَذهِ التهديدات دراستها وفهمها، والاعتراف بها كفجوة تَقنية تَزداد وبشكَل مستدام يومياً بَينَ خُبراء الامن السيبراني، ومن ثم يَنبغي عليهم تطبيق البرامج التوعوية بالهجمات السيبرانية ومنعها، وتطبيق برامج توعوية مُكثفة للزبائن كَي لاَ يقعوا ضحية لمجرمي سرَقة المعلومات والبيانات الحساسة. وفي أطار ما تَمَ سَرده سابقاً تمكنَت الباحثة مِن صِياغَة مُشكلَة البحث الرئيسة **ما هوأثر إدراك الزبون بالاختراق الرقمي كوسيلة لتحقيق الأمن السيبراني؟**، وعرض الأسئلة الفرعية على النحو الآتي:

1. ما مدى علاَقة إدراك الزبون بالاختراق الرقمي بأحداث التغييرات في بيئة الأمن السيبراني
2. كيف تؤثر الهجمات السيبرانية كالاختراق الرقمي في ظهور أنماط جديدة للصراعات الرقمية؟
3. لأي مدى يمكننا الإحاطة في ظاهرة إدراك الزبون، والعمل على مواجهة هذهِ الظاهرة والحد من ظاهرة الاختراق الرقمي في مصرف الرافدين، ومدى تأثيره في دعم الأمن السيبراني؟
4. هَل يمكننا الحد مِنَ الهجمات السيبرانية بالفضاء السيبراني؟

ثانياً؟ أهمية البحث:

1. معرفة ظاهرة الاختراق الرقمي لكونها احدى التهديدات الناتجة عن استخدام التكنولوجيا الحديثة واتباع الطرق والبرامج للحد منها.

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (1): 79-94
Doi: www.doi.org/10.25130/tjaes.22.SP7.1.5

2. جاءت أهمية البحث من منطلق ولادَة مرحلة جديدة بنظم المعلومات المصرفية بعدها ظاهرة اقتصادية واجتماعية وإنسانية لا يمكنها أن تتطور بذاتها.

ثالثاً. اهداف البحث:

1. إدراك وعي الأفراد العاملين في مصرف الرافدين بالاختراق الرقمي وحث الزبائن على تفعيل أنظمة الحماية العالمية لتجسيد آلية الأمن السيبراني.
2. التعرف على علاقَة الاختراق الرقمي في أحداث التغيرات في بيئة الأمن السيبراني.
3. التعرف على أثر الهجمات السيبرانية كالاختراق الرقمي في بروز انماطاً جديدة للصراعات السيبرانية.
4. التعرق على إمكانية المصارف في الحد من الهجمات السيبرانية في الفضاء الرقمي.

رابعاً. فرضيات البحث: لكي يمكننا الإجابة عن أسئلة البحث، تمكنا مِن صياغَة فرضية رئيسية كالآتي:

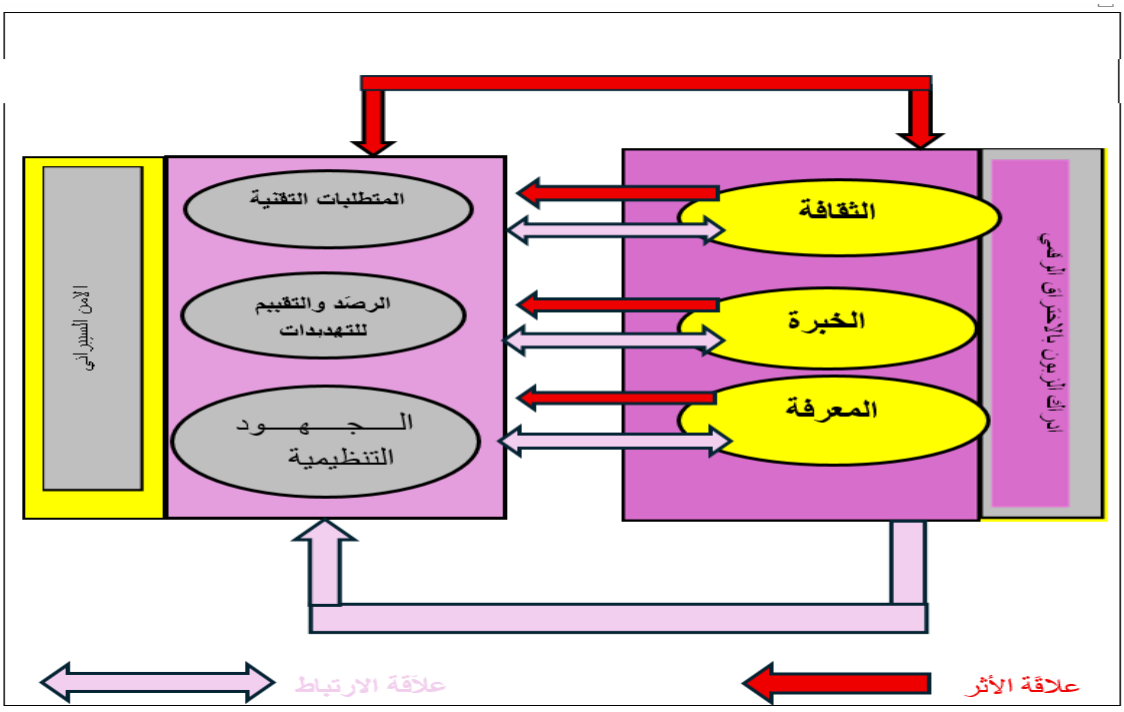
❖ **هَل هنالكَ علاقة تَأثير وعلاقة ارتباط ذات دلاَلةً إحصائية مَعنوية بَين إدراك الزبون بالاختراق الرقمي حولَ واقَع الأمن السيبراني.** وتفرعت الفرضية الى فرضيات ثلاث فرعية كالآتي:

H1: هُنالكَ علاقَة تَأثير وارتباط مَعنوي إيجابي لأدراك الزبون بالاختراق الرقمي (للمتطلبات التقنية) في الأمن السيبراني بالدِراسة.

H2: يوجَد علاقَة تَأثير وارتباط معنوي لإدراك الزبون بالاختراق الرقمي على (للرصَد وتقييم التهديدات) في الأمن السيبراني بالدِراسة.

H3: هُنالكَ علاقَة تَأثير وارتباط معنويً ايجابيً الادراك الزبون بالاختراق الرقمي (للجهود التنظيمية) في الأمن السيبراني بالدِراسة.

رابعاً. مخطط البحث:



شكل (1): مخطط البحث، مِن إعداد الباحثة

خامساً. منهج البحث: لغرض الوصول إلى المعلومات الملائمة في اجراء البحث اعتمدا الباحثون المنهج الميداني مِنَ خلال الاطلاع على المصادر الأجنبية والعربية، من مجلات ورسائل واطاريح، لوصف متغيرات البحث، ولإستنباط هذهِ المتغيرات استخدمت الباحثة استمارة الاستِبانة للِقياس، والتحليل للوصول إلى النتائج المنطقية التي تدعم فرضيات البحث، وللتعرف على مدى إدراك الزبون بالاختراق الرقمي وأثرها كوسيلة لتحقيق الأمَن السيبراني في القطاع المصرفي، لتحليل بياناتها، وإيجاد العلاقة بينَ مكوناتها' والآراء المطروحة منها حولَ العمليات، يوضحها الجدول الآتي:

جدول (1): مُتغيرات الدِراسة الواردة بالاستبانة

ت	المتغيرات الرئيسية	المتغيرات الفرعية	عدد الفقرات	ارقام الفقرات	المصادر
1	الخصائص الديمغرافية	مصرف الرافدين، الجنس، العمر، المستوى التعليمي، نوع الوظيفة	5	5	بتصرف عن الباحث
2	ادراك الزبون بالاختراق الرقمي	الثقافة	10	X1-X10	بتصرف الباحث بالاعتماد على الجانب النظري
		الخبرة			
		المعرفة			
3	الامن السيبراني	المتطلبات التقنية	6	X11-X16	الاعتماد على الجانب النظري و(Karthikeyan,2023)
		الرصد والتقييم والتهديدات	6	X17-X22	
		الجهود التنظيمية	5	X23-X27	

المصدر: من اعداد الباحثة بالاعتماد على استمارة الاستبانة.

سادساً. وصف عينة البحث ومبررات الاختيار: أن عملية اختيار ميدان الدراسة وملائمتها تعد من المحاور المهمة للبحث العلمي لأنها تسهم بشكل فعال في صحة النتائج واختبار الفرضيات ومن خلال الجانب النظري والميداني للدراسة، فَمن الضروري تسليط الضوء وغرس الثقافة لدى الزبائن بهذه المفاهيم وتوعيتهم بالاختراق الرقمي وذلك لتحقيق الأمن السيبراني وخصوصا بعد التطور الحاصل في القرن العشرين وزيادة التعاملات الرقمية باستخدام الحاسوب عن طريق الشبكة العنكبوتية في اغلب التعاملات المصرفية وغير المصرفية، سيتناول هذ المبحث وصفا شاملا لميدان الدراسة والمتمثل في مصرف الرافدين ووصف وتشخيص عينة الدراسة والمتمثلة بالزبائن المتعاملين مع هذا المصرف (جميع الزبائن غير محدد)، كما إن وصف وتحديد مشكلة الدراسة وفهمها وتفسيرها يعد من الأهداف الرئيسة لأي بحث علمي الأمر الذي يتطلب التعرف على موقع عملها وكيفية اختيار المجتمع الذي تنتمي آلية، فضلا عن تهيئة وتصميم عينة الدراسة والتي تمثل مستودع البيانات التي يستفاد منها الباحث في اجراء التحليل الاحصائي للوصول إلى النتائج النهائية وبناءً على ما تقدم تم اختيار مصرف الرافدين ميدانا للبحث لمبررات عدة أهمها:

1. الدور الحيوي والمهم لمصرف الرافدين في تقديم أفضل الخدمات وتوعية الزبائن بالاختراق الرقمي.

2. لمصرف الرافدين الدور الأكبر والفعال لتحقيق الأمن السيبراني وذلك لأنه معاملاته اليومية مع أصحاب المصلحة تكون ذات طابع حساس جدا فيما يخص العمليات المصرفية النقدية وغير النقدية.
3. عدم وجود بحوث حد علم الباحث التي حاولت اختبار أثر إدراك الزبون بالاختراق الرقمي كوسيله لتحقيق الأمن السيبراني.
4. للتحولات التكنلوجية المتسارعة وانتشار استخدام الشبكة العنكبوتية وزيادة حدة المنافسة بين المصارف للحصول إلى حصة سوقية عالية حتمت على المصارف اللجوء إلى وضع قيود واجراءات لتوعية الزبون بالاختراق الرقمي، لتتمكن من تطوير وبناء مقدرات تنافسية تمكن المصارف من وضع خيارات استباقيه لمنع وقوع الهجمات عبر الشبكة العنكبوتية لتحقيق الأمن السيبراني.

سابعاً. وصف عينة البحث: يشمل مجتمع البحث أصحاب المصلحة كافة المتعاملين مع مصرف الرافدين في حين تضمنت عينة الدراسة بعض الزبائن المتعاملين مع مصرف الرافدين بفرعيه الخاصة بتكريت وقضاء الدور مجالا تطبيقيا للدراسة حيث قام الباحثين بتوزيع 50 استبانة كان المسترجع منها 40 استبانة وبنسبة 80%، ويصف الجدول رقم (4) مفردات عينة البحث المختارة لمصرف الرافدين والخاص بالمعلومات الشخصية حسب المتغيرات الديمغرافية المختارة وكالآتي:

جدول (2): وصف عينة الدراسة

المتغيرات	الوصف	التكرارات	النسب المئوية %
الجنس	ذكر	32	80
	انثى	8	20
	المجموع	40	100
العمر	30 -20	4	10
	40-30	14	35
	50-40	12	30
	50 فأكثر	10	25
	المجموع	40	100
المستوى التعليمي	متوسطة	5	12.5
	اعدادية	8	20
	دبلوم	7	17.5
	بكالوريوس	11	27.5
	شهادة عليا	9	22.5
	المجموع	40	100
نوع الوظيفة	موظف دائم	23	57.5
	عقد	12	30
	اجر يومي	5	12.5
	المجموع	40	100

المصدر: من اعداد الباحثة بالاعتماد على برنامج (SPSS).

1. الجنس: يتبين أن الذكور شكلوا نسبة 80% من حجم أفراد العينة والبالغة والبالغة (N=40) وهي النسبة الأعلى، في حين إن نسبة النساء لم تتجاوز (20%) حيث بلغت أقل من ربع العينة وهذا يعكس واقع التعاملات المصرفة.
2. العمر: يمكن ملاحظة أن الفئة الشبابية والتي تقع ضمن فئة عمرية (20-30) سنة تشكل الفئة الاقل وبنسبة 10% وهذا يعني أن غابية أفراد العينة هم من الذين تجاوزت أعمارهم 30 سنة، مما يرجح النضج الفكري للإجابة على عبارات الاستبانة.
3. التحصيل الدراسي: من الجدول أعلاه الخاص بالمتغيرات الديمغرافية يلاحظ الفئة الأكثر استجابة هم من حملة شهادة البكالوريوس بنسبة 30% يليهم حملة الشهادات العليا بنسه 22.5% وبعد ذلك شهادات الدبلوم (المعاهد) بنسبه 20% ثم الاعدادية بنسبة 17.5% واخيرا شهادة المتوسطة وهي النسبة الاقل حيث بلغت 10% وهذا يعكس دقة الاجابات على فقرات الاستبانة.
4. نوع الوظيفة: كانت النسبة الأعلى للإجابة عن فقرات الاستبانة للموظفين وبنسبة 57.5 تليها اجابات العقود بنسبة 30% وأخيرا الأجر اليومي أذ شكلت اجاباتهم نسبة 12.5% وهذ يشير إلى أن الموظفين على الملاك الدائم هم الأكثر تعاملا مع المصارف الحكومية.

ثامناً. حدود الدِراسة:

- **الحدود الموضوعية:** اقتصرت الدِراسة على العلاقة بينَ مُتغيراتها (الثقافة- الخبرة- المعرفة) والمتغير التابع (المتطلبات التقنية- الرصد والتقييم للتهديدات- الجهود التنظيمية).
- **الحدود المكانية**: عدد من فروع مصرف الرافدين والمتمثلة بمصرف الرافدين الخاص بتكريت وقضاء الدور.
- **الحدود الزمانيةِ:** من 1/ 6 إلى فترة نهاية الدِراسة.
- **الحدود البشرية:** تمثلت الحدود البشرية، في الزبائن المتعاملين مع مصرف الرافدين للفرعين المذكورين تكريت وقضاء الدور.

المبحث الثاني: الخلفية النظرية لمتغيرات البحث

أولاً. إدراك الزبون بالاختراق الرقمي:

1. **المفهوم:** يشهد العصر الحالي ثورة معلوماتية كبيرة أثرت وبشكل مباشر بحياة الفرد شكلً ومضموناً، وإن أيجاد بيئة اجتماعية لم يكن مألوفا قبَل أن يُطلَق عليها البيئة الافتراضية أو الرَقمية. فأصبحت وسيلة لكثير مِن الممارسات والعلاقات والأنشطة، وقَد رافق هذهِ الأنشطة أفعالً عدة والتي شكلت فعلاً اجرامياً بحكم القانون والتي أطلق عليها الجرائم الرقمية أو الاختراق الرقمي وهي من الجرائم العصرية الحديثة والتي ظهرت مع تطور الحياة الاقتصادية ووصول المجتمع لعصر التقانة والمعلوماتية، بزمنً أصبح فيه الاقتصاد والأمن من متطلبات حياة الأعمال، وتشكل هذهِ الأنشطة المستحدثة العديد من الضحايا (بن عزوز وحليمة، 2022: 582).

وانتشرت هذهِ الظاهرة انتشارا واسعاً بوقتً قياسِ فأصبحَ مستخدميها بمستويات تعليمية مختلفة وبكافة الفئات العمرية، وعرفها (Karthikeyah, 2023: 460) بأنها حجر الأساس في مواجهة الاحتيال والنصب والحد من أثارها، أما (علي، 2019: 7) فيرى بأن إدراك الزبون للاختراق الرقمي بأنه القدرة على صنع القرارات الفعالة والالمام الشامل بالتحديات والقضايا المتعلقة بأداة الثروة والنقد والتي تجعل القطاع المالي ذو فعالية أكبر في صنع القرار المالي.

وترى الباحثة بأن إدراك الزبون بالاختراق الرقمي (الافتراضات والمعارف والمواقف والمعايير والقيم التي يتحلى بها المستخدم في أي مؤسسة مالية والتي تحدد كيفية تفكير الافراد فيما يتعلق بالوصول غير المصرح به من قبل الاجندة الخارجية المتطفلة المعلومات المالية والشخصية بمختلف الوسائل والتعامل معها).

2. **أهمية إدراك الاختراق الرقمي:** تكمن أهمية الأدراك بالعمَل المصرفي (محمد، 2019: 10)، (التوني، 2023: 630)، في الآتي:

- ❖ مَقدرة الزبون على فهَم آلية العمل المصرفي.
- ❖ التقدَم التقني والشبكات المعلوماتية والخدمة المصرفية المتعددة يتطلب الاستجابة السليمة للوقت والمسؤوليات للتعامل مع الخدمات من قبا أصحاب المصلحة في المصرف.
- ❖ يعد النقد أحد مظاهر استيقاظ الادراك، والمحدد للبنى الفكرية عند صقلها وجعلها في حالة من الاشعاع والتوهج.

3. **متطلبات إدراك الزبون بالاختراق الرقمي** (Rammal, 2020: 8), (Chaudhry, et al, 2011: 3):

- ❖ **التنوع:** تَقديم التعليم
- ❖ **المشاركة:** التعاون مع الآخرين لأهمية إدراك الاختراق الرقمي.
- ❖ **الشمولية:** الوصول إلى جميع أصحاب المصلحة الأكثر احتياجاَ للأجيال المستقبلية للمستثمرين والمستهلكين.

4. أبعاد إدراك الزبون للاختراق الرقمي:

- ❖ **الثقافة:** تشير إلى تثقيف الموارد البشرية بأهمية أمان وحماية البيانات وممارسات التسجيل والدخول الآمن من التهديد السيبراني، فضلاً عِن اعتماد كلمات مرور قوية واتخاذ أفضل السياسات للتعامل الآمن مع الأنظمة والبيانات.
- ❖ **الخبرة:** امكانية الزبون (مؤسسة أو فرد) في التعامل مع الهجمات السيبرانية المختلفة، من خلال معرفته بالتهديدات وأساليب الوقاية منها، والإجراءات المتخذة عند الوقوع فيها.
- ❖ **المعرفة:** تشير إلى الوسيلة التي توحد بها المؤسسة التكنولوجيا مع إدارة المعرفة لِمساعدتهم على فهم الزبون والتعامل معه في كيفية فهم وأدراك أخطار الاختراق الرقم (A, 2017: 7)، (فرج، 2021: 543).

ثانياً. الأمن السيبراني:

1. **الأمن السيبراني:** ينقسم مصطلح Cybersecurity على كلمتين الأولى (الامن) والثانية (CYBER) السيبراني والذي يتمحور في الأساس حول مفهوم الأمن، كالأمن المرتبط بالشبكة العنكبوتية لحمايتها من cyber attack والتي يكون مصدرها الأشخاص او التنظيمات وحتى الحكومات، وتعمل على تحقيق الحفاظ على Cybersecurity عن طريق توفير The most (modern protection programs) من الهجمات السيبرانية المختلفة (كهجمات التجسس المالي والاقتصادي) للهيمنة على المعلومات والبيانات المتعلقة بالمصارف والزبائن (Rahman, 2023: 2).
2. **مفهوم الامن السيبراني:** الأمن السيبراني هو عملية تأمين أنظمة الحاسوب والشبكات والبيانات من الوصول غير المرغوب فيه، والسرقة، والتلف، أو الانقطاع. ويشمل استخدام التقنيات والأساليب والسياسات لحماية أنظمة الحاسوب والشبكات من التهديدات السيبرانية، مثل الفيروسات والبرامج الضارة والقرصنة وهجمات التصيد الاحتيالي، فضلا عن ضمان سرية البيانات والمعلومات الحساسة

وتوافرها. ويهدف الأمن السيبراني إلى تجنب أو الحد من الضرر الناجم عن الحوادث الأمنية، وحماية خصوصية المعلومات الحساسة وأمنها، وضمان استمرارية العمليات التجارية (المالية) الحيوية (Dawodu& Omotosho, 2023: 5)

3. أنواع الامن السيبراني:

❖ **أمن المعلومات (أو InfoSec):** هو عملية تصميم ونشر أدوات لحماية معلومات أعمالك المهمة من التدمير والتعطيل والتغيير. وهو عامل حاسم في الأمن السيبراني، حيث صُمم خصيصًا لأمن البيانات. الهدف الرئيس لأمن المعلومات هو سرية بيانات أعمالك وسلامتها وتوافرها (CIA). صُمم هذا الأمن لضمان وصول المستخدمين أو التطبيقات أو الأنظمة المصرح لها فقط إلى معلومات معينة. وفيما يلي أنواع أمن المعلومات:

- **أمن السحابة:** يركز بشكل رئيس على الثغرات الأمنية الناتجة عن خدمات الإنترنت والبيئات المشتركة. يحمي أمن التطبيقات والبنية التحتية من المكونات المتصلة بالسحابة.
- **التشفير:** عملية حجب المحتوى لتأمين المعلومات، ولا يمكن الوصول إلى البيانات المشفرة إلا من قِبل المستخدم الذي يمتلك مفتاح التشفير الصحيح. يحافظ التشفير على سرية البيانات وسلامتها أثناء نقلها وتخزينها.
- **إدارة الثغرات الأمنية:** هذا النوع من أمن المعلومات هو عملية تُفحص فيها البيئة بحثًا عن أي نقاط ضعف، مثل البرامج غير المُرقعة. بالنسبة للشركات الناشئة التي تُضيف باستمرار مستخدمين أو تطبيقات أو تحديثات جديدة للبنية التحتية، يُعد هذا عاملًا مهمًا لمراقبة المخاطر المحتملة.

❖ **الأمن التشغيلي Operational Security:** وتشير إلى القرارات والعمليات ذات العلاقة بمعالجة وحماية البيانات، فضلاً عن الأذونات التي يحتاج إليها المستخدمون لغرض الوصول إلى الإجراءات الخاصة في مكان وكيفية خزن ومشاركة المعلومات (DARCY & Rahman, 2023: 2) (Basogtu, 2022: 10).

4. **المعايير المطلوبة للأمن السيبراني:** نتيجة لتفاوت أهمية المعلومات، ودرجة سريتها للحفاظ عليها لذي فمن الصعب وضع نظم قياس لتصنيف هذه المعلومات التي تغطي جميع الإجراءات المطلوبة لتكون ملائمة للمواقف جميعها، فمثلاً هُنالك معلومات تخضع المؤسسات المالية والمصرفية والتي يترصَد المنافسين لها لعرقلة سير عملياتهم، وتوظيفها لصالحهم، ومن أهم هذهِ المعلومات:

- **أسرار المؤسسة الداخلية:** تقع ضمن محيط الدائرة السرية المطلقة والتي ينبغي حمايتها بدقة فائقة. لكونها تكشف موقع المؤسسة وامكانيتها المالية.
- **المعلومات المالية:** والتي غالباً ما يهتم بها أصحاب ورؤوس أموال المؤسسة للتأكد من سلامة ودقة هذهِ المعلومات من خلال الفحص الدوري لِضمان درجة الحماية القصوى لها.
- **المعلومات المرتبطة بالمورد البشري:** وتشير إلى حماية المعلومات المتعلقة بالأفراد العاملين في المصرف (البيانات الشخصية للموظف كالرواتب والتقارير الصادرة والتامين) (kalunda, 2019: 10) (الشيخ والحنيطي، 2023: 11).

5. متطلبات تحقيق الأمن السيبراني:

❖ **البريد الاحتيالي:** ويشير إلى عدم النقَر فوق روابط الرسالة مجهولة الهوية أو فتح مرَفق البريد الرقمي.

❖ **النسخ الاحتياطي:** تهدف إلى عمل نسخ الملفات الاحتياطية المنظمة لمنع هجمات الأمن على الشبكة العنكبوتية.

❖ **الموثوقية:** تعمل على استخدام مواقع موثوقة عَند تقديم المعلومات الشخصية والقاعدة الرئيسية هي التحقق من عنوان (URL) فعندما يحتوي الموقع على https فهو آمن والعكس صحيح (مجاهد، 2023: 64) (Aqeel, et al., 2019: 20).

6. أبعاد الأمن السيبراني:

❖ **المتطلبات التقنية:** وتشير إلى الفهم العميق للأنظمة والشبكات، والمعرفة الواسعة فيما يتعلق بالاختراق الرقمي والقرصنة الأخلاقية، واتقان اللغات، فضلاً عِن القدرة على إدارة النظم الحاسوبية المختلفة ومنها جار الحماية، والتشفير، والتقانات المستخدمة.

❖ **الرصَد والتقييم للتهديدات:** أحد الوسائل المستدامة في مراقبة وتحليل الأنظمة والأنشطة، للكشف عن الحوادث الأمنية، والتجاوزات المرتقبة، الأمر الذي يساعد المؤسسة في اتخاذ الاجراء الاستباقي لحماية الأنظمة والبيانات.

❖ **الجهود التنظيمية:** آلية لوضع الإجراءات والسياسات والمعايير والأنظمة لِضمان حمايَة البيانات والأصول الرقمية من التهديد السيبراني (Kalakuntia, et al, 2019: 117)، (Seema, at el., 2018: 128)

المبحث الثالث: الجاني العملي

نتائج اختبار الارتباط

جدول (3): نتائج اختبار الارتباط

التفسير	R^2 (%)	95% CI	Df	قيمةt	قيمة p	معامل الارتباط (r)	الفرضية
ارتباط موجب متوسط القوة ودال إحصائيًا	17.6	[0.12, 0.65]	38	2.85	0.007	0.42	H1: إدراك الزبون ↔ المتطلبات التقنية
ارتباط موجب متوسط القوة ودال إحصائيًا	14.4	[0.08, 0.62]	38	2.52	0.016	0.38	H2: إدراك الزبون ↔ الرصد والتقييم
ارتباط ضعيف وغير دال إحصائيًا	8.4	[-0.03, 0.56]	38	1.85	0.072	0.29	H3: إدراك الزبون ↔ الجهود التنظيمية

تفسير النتائج:

❖ الفرضية الأولى (H1): أظهرت النتائج أن قيمة معامل الارتباط (r=0.42) عند مستوى دلالة (p=0.007) تمثل علاقة ارتباط موجبة متوسطة القوة بين إدراك الزبون بالاختراق الرقمي والمتطلبات التقنية للأمن السيبراني. أي أن زيادة وعي الزبون أو إدراكه بتهديدات الاختراق ترتبط بزيادة الحاجة إلى تعزيز المتطلبات التقنية. هذا يعكس أن المؤسسات التي يزداد وعي عملائها بالاختراقات الرقمية تكون مضطرة لتطوير بنيتها التحتية الأمنية بشكل أكبر.

- الفرضية الثانية (H2): العلاقة هنا (r=0.38, p=0.016) تؤكد ارتباطًا إيجابيًا متوسطًا بين إدراك الزبون بالاختراق الرقمي والرصد والتقييم الأمني. هذا يعني أن وعي الزبائن يسهم في تعزيز قدرة المؤسسات على الرصد والتحليل المبكر للتهديدات. وهو ما يشير إلى أن مشاركة الزبائن في الإبلاغ عن محاولات أو مؤشرات الاختراق ترفع من فعالية أنظمة الرصد.
- الفرضية الثالثة (H3): بالرغم من وجود ارتباط موجب ضعيف (r=0.29)، إلا أن قيمة(p=0.072) غير معنوية إحصائيًا. هذا يدل على أن إدراك الزبون لا يرتبط بشكل واضح أو مؤثر بالجهود التنظيمية الداخلية. تفسير ذلك أن الجهود التنظيمية عادة تعتمد أكثر على سياسات الإدارة والموارد الداخلية وليس على إدراك الزبون مباشرة.

نتائج اختبار التأثير (الانحدار البسيط):

جدول (4): نتائج اختبار التأثير (الانحدار البسيط)

الفرضية	t	F	β (Standardized)	B (Unstandardized)	Sig. (p)	القرار
H1: إدراك الزبون → المتطلبات التقنية	2.85	8.12	0.42	≈0.42	0.007	مقبولة
H2: إدراك الزبون → الرصد والتقييم	2.52	6.35	0.38	≈0.38	0.016	مقبولة
H3: إدراك الزبون → الجهود التنظيمية	1.85	3.42	0.29	≈0.29	0.072	مرفوضة

تفسير النتائج

- الفرضية الأولى :(H1) قيمة t=2.85 و F=8.12عند مستوى دلالة (p=0.007) تشير إلى وجود تأثير معنوي. قيمة β=0.42 تعني أن التأثير متوسط، وكل زيادة وحدة في إدراك الزبون تؤدي إلى زيادة مباشرة في المتطلبات التقنية. هذا يبرز أن إدراك الزبون عامل مهم في دفع المؤسسات نحو تطوير أمنها السيبراني.
- الفرضية الثانية :(H2) قيمة t=2.52 و(p=0.016) F=6.35 تدل على تأثير معنوي متوسط القوة. قيمة β=0.38 توضح أن إدراك الزبون يسهم في تفسير 14.4% من التباين في قدرات الرصد والتقييم. هذا يعني أن وعي الزبون يعزز فعالية المؤسسات في التعامل مع التهديدات.
- الفرضية الثالثة :(H3) قيمة t=1.85 و F=3.42لم تكن معنوية .(p=0.072) ورغم أن قيمة β=0.29 تشير إلى تأثير ضعيف، إلا أن هذا التأثير لا يصل لمستوى الدلالة المطلوبة. بالتالي، الإدراك لا يشكل عاملًا قويًا في التأثير على الجهود التنظيمية، والتي غالبًا تتأثر بقيادة الإدارة العليا والسياسات المؤسسية أكثر من الزبائن.

وبشكل عام تبين الآتي:

1. الإدراك الرقمي للزبون يُعد متغيرًا مهمًا في تفسير جانب من المتطلبات التقنية وقدرات الرصد والتقييم.
2. التأثير في الجهود التنظيمية لم يظهر واضحًا، ما يعكس أن هذه الجهود تعتمد أكثر على السياسات الإدارية الداخلية وليس على وعي الزبون.
3. حجم الأثر (Effect Size) كان متوسطًا في الفرضيتين الأولى والثانية، وضعيفًا في الثالثة.

المبحث الرابع: الاستنتاجات والتوصيات

أولاً. الاستنتاجات:

1. انطلاقاً مِن طبيعة الاختراق الرقمي المتطور وغير القابَل للتنظيم المحدد، مع إمكانية معالجة القضايا المتعلقة بالاحتيال الرقمي مِن خلال استخدام اللوائح المتعلقة بمخاطَر التقانات المستخدمة والمخاطَر التشغيلية.
2. التطوَر المستدام لِمجرمي البيئة الافتراضية حفزَ المؤسسات المالية والمصرفية وخاصَةً مصرف الرافدين البحث باستمرار لإتخاذ الإجراءات الوقائية ضَد المخاطَر السيبرانية مِن خلال عرضها في برامج التوعية لجعلها واضحة أمام مجلس إدارة مصرف الرافدين، مما يؤدي لدعم الاستقرار المالي للمصرف.
3. توسيع قاعدَة مهارات الموارد البشرية الرقمية، فضلاً عَن اجتذاب المختصين في مجال الأمِن السيبراني للتعامَل معَ الهجمات السيبرانية.

ثانياً. التوصيات:

1. يعد فهم الأمن السيبراني وكيفية تطبيقه أمرًا بالغ الأهمية في مجتمع اليوم المُعتمد على التكنولوجيا والشبكات. فبدون وجود ضمانات مناسبة، تُصبح الأنظمة والملفات والبيانات المهمة والأصول الرقمية الأخرى عُرضة للاختراق. لذا، فإن مستوى الأمان نفسه مطلوب لجميع المؤسسات، بغض النظر عن تخصصها في تكنولوجيا المعلومات.
2. تُشكل البيانات المالية، والمعلومات الشخصية، وأنواع أخرى من البيانات التي قد يُؤدي الوصول إليها أو الاطلاع عليها غير المصرح به إلى مخاوف سلبية على أمن وخصوصية المصرف.
3. ضرورة زيادة التعاون المشترك بين المصارف الحكومية والمصارف الأهلية من أجل تحسن وتطوير استراتيجية الأمن السيبراني.
4. اعتماد استراتيجية الامن السيبراني كرأس هرم للحد من الجرائم المصرفية من خلال تطوير البنية التنظيمية والإدارية والتقنية في إدارة الأمن السيبراني.

المصادر

1. الحديدي، شيرين إسماعيل خليل محمد، (2024)، "(مهارات القيادة الرقمية وتأثيرها في الحد مِنَ هجمات الهندسة الاجتماعية/ الدور الوسيط للمواطنة الرقمية- دراسة تحليلية لآراء عينة من العاملين لشركات الاتصالات الخلوية العراقية")، أطروحة دكتوراه، جامعة تكريت، كلية الإدارة والاقتصاد.
2. الشيخ، جميل سعيد جميل، الحنطي، هناء محمد، (2023)" (دور محددات الامن السيبراني في الاشتمال المالي في البنوك الإسلامية العاملة في الأردن)"، المجلة الدولية للعلوم الإنسانية والاجتماعية، العدد(52)، DOI: https://doi.org/10.33193/IJoHSS.52.2023.650.

3. مجاهد، فايزة احمد الحسيني، (2023)، "(الوعي بالامن السيبراني ترف ام ضرورة في عصر المعلوماتية)"، مجلة بحث وتربية المعهد الوطني للبحث في التربية، المجلد (13)، العدد (02)، ص ص 54- 74.
4. فرج، علياء عمر كامل، (2021)، "(دواعي تعزيز ثقافة الامن السيبراني في ظل التحول الرقمي جامعة الأمير سطام بن عبد العزيز نموذجاً)"، جامعة سوهاج، كلية التربية، المجلة التربوية، عدد فبراير- ج1- (94).
5. السمحان، منى عبدالله، (2020)، "(متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود)"، مجلة كلية التربية- جامعة المنصورة- العدد(111).
6. بن عزوز، حاتم، حليمة، مناني، (2022)"(الامن السيبراني والجريمة الالكترونية في الدول ما بعد الحداثية: الولايات المتحدة الامريكية – نموجا)"، مجلة الرسالة للدراسات الإعلامية، المجلد(06)، العدد(02)جوان، 2022. ص ص 580- 589.

ثانياً. المصادر الأجنبية:

1. Rahman Mdhsnur (2023),"(An In-Depth Analysis of Cybersecurity)", School of Electronics and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. North American Academic Research. 2023, 6(2), https://doi.org/10.5281/zenodo.7698121 Monthly Journal by TWASP, USA NAAR Home (twasp.info) NAAR, February 2023, Volume 6, Issue 2, 45-53.
2. D'Arcy, J. and Basoglu, K. A. 2022.)"The influences of public and institutional pressure on firms' cybersecurity disclosures"). Journal of the Association for Information Systems. 23(3): 779-805. https://doi.org/10.17705/1jais.00740.
3. Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O. and Ewuga, S. K.)2023)." (Cybers. ecurity risk assessment in banking: methodologies and best practices. Computer)" 975 Science and It Research Journal, 4(3), 220-243. https://doi.org/10.51594/csitrj.v4i3.659
4. 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.
5. Bin Aqeel, Muslim., Imran, Abubakar., & Mehwish Iftikhar.)2019(("Investigating the Effect of Social Media on the Students' Academic Performance. Gomal University (Journal of Research. Jan 2019.Vol 2. N 35. Pp: 66-78.
6. Sowmiya, M, Seemma, P.S, Nandhini, S, (2018), "(overview of cyber security)", international journal of advanced research in computer and communication engineering, vol.7, lessee, November.
7. Kalakuntla, Rothit, Vanamala Anvesh Babu, Kolipyaka Ranjith Reddy, (2019), "(cyber security)" Hora Asociatia Holistica Rfsfarch Acadfmic, Vol(10)lssue 2, 2019.PP.115-128.
8. 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.
9. Fortin, Anne and Heroux, S., (2023), "(Cybersecurity disclosure by the companies on the SPP/TSX60)", index, vol:19, issue:2, June, pp:73-102.

10. El Hissi, Y.& Arezki, S.(2018) "(.Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in Moroccan University)",2018 4th International Conference on Computer and Technology Applications.
11. Almutairi, Bandar S, Alghamdi, Abdurahman, (2022), "(The Role of Social Engineering Cybersecuity And Its Impat)", Journal of Information Security, Dol: 10. 4236/ jis.2022. 134020 Oct.28,2022. Aldawood, H., & Skinner, G. (2018). "(Educating and Raising Awareness on Cyber Security Social Engineering)": A Literature Review. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (pp. 62–68). IEEE.
12. Chaudhry, Peggy,E,S, Sohail, A, Stephen. Sudler, Hasshi,(2011)"(Iracy in Cyber Space: Consumer Complicity, Pirates and Enterprise Enforcement)" Article in Enterprise Information Systems · May 2011 DOI: 10.1080/17517575.2010.524942 · Source: DBLP, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/220478904.
13. 13.A, Karimi, &S,M,Allameh,(2017)"(Investigation the relationship between customer knowledge management and customer loyalty: mediating role of customer value (Case study: Saderat Bank of Khozestan)". New Trends &Issuues Proceedings Humanities &Social sciences,2(2).
14. 14. Rammal F. G., (2020)."(Awareness of Commercial Banking products among Customers: The case of Australia"), International journal of economics andfinance.pp147.
15. 15. Karthikeyan, L, Jaikala,(2023)"(A Study on Customer Awareness on Cyber Security and Digital Payment Fraud Prevention in Nationalized Banks (1))". Journal of Harbin Engineering University ISSN:1006-7043, VOL(44)NO(08), A Uugust (2023) See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/373217815

م/ استمارة الاستبانة

مرحباً بكم أنى الباحثة شيرين إسماعيل خليل من جامعة تكريت كلية الإدارة والاقتصاد أقوم بأجراء دراسة حولَ (أثر إدراك الزبون بالاختراق الرقمي كوسيلة لتحقيق الأمن السيبراني: دراسة ميدانية في مصرف الرافدين)، وارغبُ ان اعرف تجربتكم مع (مصرف الرافدين) ، يُرجى من حضارتكم اكمال هذهِ الاستبانة، ردودكُم مَجهولة الهوية ولا يمكنكُم تخطي الأسئلة التي لا تشعركم بالراحة اتجاهها، شاكرين لكم مُشاركتكُم.

م. د: شيرين إسماعيل خليل الحديدي م، م صباح صابر محمد الدوري

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (1): 79-94
Doi: www.doi.org/10.25130/tjaes.22.SP7.1.5

م/ الاستبانة

المحور الأول: المعلومات الديموغرافية

العمر: اقل من 30( ) من 30 الى 40( ) من 40 الى 50( ) 50 فاكثر( )

الجنس: انثى ( ) ذكر ( )

المستوى التعليمي: شهادة عليا ( ) بكالوريوس ( ) دبلوم ( ) اعدادية ( ) متوسطة ( )

نوع الوظيفة: دائم ( ) عقد ( ) اجر يومي ( )

المحور الثاني: متغيرات البحث

اولاً. المتغير المستقل: أدراك الزبون بالاختراق الرقمي: تشير الى وعي وثقافة الزبون بعملية اختراق الأجهزة الرقمية بطريقة غير قانونية من قيل القراصنة للتجسس وجمع المعلومات والمكسب المالي، كأجهزة الحاسوب، والشبكات والهواتف الذكية وغيرها (السمحان، 2020: 10).

ت	العبارة	لا اتفق	اتفق	محايد	اتفق بشدة
1	يعمل المصرف على التواصل مع أساليب الإعلان المحلية لنشر اخباره				
2	يتواصل المصرف مع الزبون ويبلغه بكافة المستجدات.				
3	يعمل المصرف على نشر التقارير المالية لتوعية الزبون مصرفياً.				
4	يتعامل المصرف مع الصحف المحلية لنشر الإعلانات بشكلً مستدام				
5	يقوم العاملين في المصرف بدورهم في نشر ثقافة الوعي المصرفي داخل وخارج العمل.				
6	يجهز المصرف ملفات عديدة لتثقيف الزبائن من الاختراق الرقمي.				
7	يمتلك المصرف موقع فعال على الشبكة العنكبوتية يحدث يومياً لنشر طرق وأساليب الاختراق الرقمي.				
8	يتواصل المصرف مع الزبون عبرَ وسائل التواصَل الاجتماعي.				
9	يعتبر المصرف هو المسؤول الأول عن حماية الزبون من الاحتيال المصرفي.				
10	يدرك أصحاب المصلحة طبيعة عمل المصرف كحلقة تواصَل بين الباحثين عن التمويل وأصحاب الأموال.				

ثانياً. المتغير التابع الامن السيبراني: يعرف أمن الحاسوب الخاص بالشبكة العنكبوتية باسم "الأمن السيبراني". الهدف الرئيسي للأمن هو منع اختراق الأجهزة من خلال تطبيق مجموعة من القواعد والإجراءات لمنع وقوع الهجمات عبرَ الشبكة العنكبوتية (ELhissi & Arezki, 2018; 14).

المتطلبات التقنية: تشير الى سعة المعرفة في استخدام تقانات وأدوات الامن السيبراني والبرمجة والشبكات ونظُم التشغيل، لِحماية البيانات الأجهزة (النظام)، والمعلومات الحساسة، والشبكات، مِن الهجمات السيبرانية (الحديدي، 2024: 120).

ت	العبارة	لا اتفق	اتفق	محايد	اتفق بشدة
1	يعمل المصرف على تحسين فاعلية الحماية باستمرار.				
2	برامج الحماية المتخصصة تتلاءم مع طبيعة العمل.				
3	تمتاز الأجهزة المستخدمة في المصرف بمواصفات عالية.				
4	يوفر المصرف البرمجيات المطلوبة للعمل بشكلٍ دوري.				
5	يمتلك المصرف لحماية البيانات والزبائن قاعدة نسخ احتياطية منتظمة لجميع المعلومات.				
6	يطور المصرف قاعدة البيانات بشكلٍ مُستدام.				

الرصد والتقييم للتهديدات: وهي عملية مُستدامة تَهدَ إلى حماية البنية التحتية للمصارف من مختلف التهديدات السيبرانية (Almutairi, Aighamdi, 2022: 365).

ت	العبارة	لا اتفق	اتفق	محايد	اتفق بشدة
1	يتفهم المصرف البنية التحتية المتعلقة بالأمن السيبراني وقدرتها.				
2	يمتلك المصرف شبكة حماية قادرة على حماية الزبون من أخطار الاختراق الرقمي التي قد يتعرضون لها.				
3	يعمل المصرف على تطوير شبكات الحماية باستمرار وتحسينها.				
4	يتبنى المصرف أنظمة حماية جديدة.				
5	يأخذ المصرف شكاوى الزبائن بعين الاعتبار.				
6	يلتزم المصرف بالقوانين ذات العلاقة بالاحتيال المصرفي.				

الجهود التنظيمية: وتشير الى حزمة من التدابير المستخدمة في حماية الزبائن وبياناتهم في المصرف مِنَ الهجمات السيبرانية وتشمَل نظُم اكتشاف ومِنع الاختراق الرقمي وجدران الحماية النارية، وبرامج مُكافحَة الفيروسات، والتشفير (ALdawood, et al., 2019: 21).

ت	العبارة	لا اتفق	اتفق	محايد	اتفق بشدة
1	اعداد وتنفيذ الاستراتيجيات المتخصصة للأمن السيبراني.				
2	استخدام نظَم حاسوبية لتطوير وتحسين الامن السيبراني				
3	تتوائم مقتضيات ومتطلبات تطوير الامن السيبراني مع الأجهزة المستخدمة.				
4	يعمل المصرف على تحديث اجهزتهُ بشكلٍ مُستدام.				
5	يستخدم المصرف برامج الحماية الحديثة				
6	يعتمد المصرف التحسين المستدام في تقديم الخدمات، فضلاً عِن قيادة أدائه والرجوع الى النتائج الفعلية وتحليلها، ثم مقارنتها مع النتائج المتوقعة في ضوء التطوير المستدام.				