

جامعة ميدأوشن



كلية الإدارة

قسم / تخصص. ماجستير إدارة مخاطر

العنوان باللغة العربية

أثر الاختراقات التقنية على الأمن السيبراني في القطاع المصرفي بالسعودية

إعداد الطالبة/وداد سلطان العنزي

إشراف/د. الفیصل عبد الحمید محمد محسن

العام الدراسي:

2024

فهرس المحتوى

الموضوع

رقم الصفحة

المحتويات..... ٢

الفصل الاول

مشكلة البحث واهميتها..... ٥

هدف البحث..... ٦

اسئلة البحث..... ٦

مصطلحات البحث..... ٦

الفصل الثاني

الاطار النظري

أولاً: المخاطر التقنية

تعريف المخاطر التقنية..... ٨

إدارة المخاطر التقنية..... ٨

المخاطر التقنية الشائعة في المصارف..... ٩

ثانياً: الأمن السيبراني

تعريف الأمن السيبراني ٩

الهجمات السيبرانية الشائعة في المصارف ٩

الآثار القانونية واقتصادية على الاختراقات التقنية على المصارف ١٠

ثالثاً: التوعية والوقاية

التدريب والتوعية بشأن الأمن السيبراني ١٠

الأدوات والتقنيات المستخدمة لرصد والوقاية من الاختراقات التقنية ١٠

الفصل الثالث

الدراسات السابقة

تحليل الدراسات السابقة ١٢

فروض البحث ١٣

الفصل الرابع

إجراءات البحث

منهج البحث ١٤

مجالات البحث ١٤

عينة البحث ١٤

أدوات البحث ١٤

الفصل الخامس

عرض ومناقشة النتائج ١٥

الفصل السادس

الاستنتاجات ١٨

التوصيات ١٨

المراجع والمصادر ١٩

ملخصات البحث

ملخص البحث باللغة العربية ١٩

ملخص البحث باللغة الإنجليزية ١٩

مستخلص البحث باللغة العربية ٢٠

مستخلص البحث باللغة الإنجليزية ٢٠

الفصل الأول

مشكله البحث:

لقد شهدت المصارف تطور تقني أتاح لها تقديم مستوى متقدم من الخدمات المقدمة للعملاء من خلال طرق مستحدثة غير تقليدية مما أدى إلى تغير جذري في طريقة عمل القطاع وفي نفس الوقت تلك الفرص تخلق العديد من التحديات والعديد من المخاطر الجديدة منها الاختراقات التقنية التي تزيد من التحديات التي يواجهها الأمن السيبراني، وهناك تحديات تتعلق بتقييم مخاطر الأمن السيبراني، بدءاً من تقدير احتمالية حدوث خرق وصولاً إلى تقدير قيمة الأصول المعرضة للخطر (دفاع للأمن السيبراني)

. هذه التحديات تتطلب من الشركات والمؤسسات تبني منهجيات مثبتة لتقييم المخاطر وتحديد الاستثمارات الإضافية المطلوبة في الدفاعات الإلكترونية ورفع التوعية لدى المستخدمين بمخاطر تبادل البيانات الشخصية المتعلقة بحساباتهم المصرفية حيث تؤثر على قدرة الأفراد والمؤسسات على البحث بشكل آمن وفعال حيث ان القطاعات المصرفية في السعودية تواجه تحديات أمنية سيبرانية متنوعة، منها:

تهديدات الاختراق والاحتيال الإلكتروني: تتعرض المؤسسات المصرفية لتهديدات مستمرة من قبل القراصنة السيبرانيين الذين يسعون للوصول إلى بيانات العملاء والمعلومات المالية من خلال اما اتصالات أو روابط مزيفة.

أهمية البحث:

أهمية بحث أثر الاختراقات الأمنية على الأمن السيبراني في القطاع المصرفي تكمن في فهم ومواجهة التحديات السيبرانية المتزايدة التي تواجهها البنوك. من خلال البحث، يمكن تحديد نقاط الضعف وتطوير استراتيجيات أمنية فعالة لحماية البيانات المالية والعمليات المصرفية. كما يساهم البحث في رفع مستوى الوعي بأهمية الأمن السيبراني وضرورة اتخاذ التدابير الوقائية والتكنولوجية للحفاظ على سلامة البيانات وثقة العملاء.

أهداف البحث:

فهم عمق التأثير: تحليل تأثير الاختراقات التقنية على أمان البيانات والعمليات المصرفية لفهم الخسائر المحتملة للعملاء.

تطوير استراتيجيات الوقاية: وضع استراتيجيات وقائية محددة لتعزيز أمان المعلومات والوقاية من التهديدات السيبرانية في القطاع المصرفي.

رفع التوعية لدى العملاء: وضع إجراءات توعية فعالة للتعامل مع حالات تحاللات محاولة الاختراق المحتملة والحد من التأثيرات السلبية.

أسئلة البحث:

- (١) ما هي أبرز أنواع الاختراقات الأمنية التي تواجهها البنوك والمؤسسات المالية؟
- (٢) كيف يمكن للاختراقات الأمنية التأثير على سلامة المعلومات المصرفية وخصوصية العملاء؟
- (٣) ما هي الثغرات الشائعة التي يستغلها المهاجمون للوصول إلى البيانات المصرفية؟
- (٥) كيف يمكن للتدريب والتوعية بشأن الأمن السيبراني أن يساهم في تقليل مخاطر الاختراقات الأمنية في القطاع المصرفي؟

مصطلحات البحث:

- الأمن السيبراني: هو مجال يهتم بحماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية والهجمات الإلكترونية.
- الثغرات التقنية: هي النقاط الضعيفة في أنظمة الحاسوب أو البرمجيات التي يمكن استغلالها من قبل المهاجمين للوصول إلى البيانات أو تعطيل الخدمات.
- التهديدات السيبرانية: يشير إلى محاولة لفضح أو تغيير أو تعطيل أو تدمير أو سرقة أو الحصول على وصول غير مصرح به للأصول.

الحماية السيبرانية: تبني تدابير وأدوات الأمن السيبراني لحماية البيانات الحساسة من الوصول غير المصرح به ومنع أي انقطاع للعمليات.

التشفير: يشير إلى عملية تحويل البيانات من صيغة قابلة للقراءة إلى شكل مشفر أو مشفر بطريقة تجعلها غير قابلة للقراءة أو الفهم لأي شخص غير مخول.

حماية البيانات الشخصية: تشير إلى عملية حماية المعلومات التي تتعلق بالأفراد والتي يمكن تحديدها أو ترتبط بشخص معين، مثل الاسم، العنوان، الجنس، العمر، أو رقم التعريف وتهدف إلى ضمان سرية وسلامة هذه المعلومات ومنع وصول غير مصرح به لها.

سياسات الأمن السيبراني: مجموعة من السياسات والإجراءات التي تهدف إلى حماية الأصول المعلوماتية والتقنية للمؤسسات من التهديدات السيبرانية.

تحليل سلوك المستخدمين: هو عملية استخدام مبادئ سلوكية لفهم وتحليل كيفية تفاعل المستخدمين مع المواقع الرقمية والتطبيقات.

الرصد والاستجابة السيبرانية: عملية مراقبة ومتابعة الأنظمة والشبكات الرقمية لاكتشاف أي أنشطة غير مصرح بها أو تهديدات سيبرانية، واتخاذ إجراءات فورية.

الفصل الثاني

تعريف المخاطر التقنية

تعني تحديد وتقييم المخاطر المحتملة التي تواجه المؤسسات في مجال التكنولوجيا والمعلومات، وتطبيق سياسات وإجراءات للتعامل مع هذه المخاطر بشكل فعال. تهدف هذه العملية إلى تقليل الآثار السلبية المحتملة على الأنظمة والبيانات التقنية، وضمان استمرارية العمل بشكل آمن وفعال.

إدارة المخاطر التقنية:

لتنفيذ خطة الاستجابة للمخاطر التقنية، يمكن اتباع الخطوات الأساسية التالية وفق المصادر المقدمة:

تحديد المخاطر: يجب تحديد المخاطر التقنية المحتملة التي يمكن أن تواجه المؤسسة في مجال التكنولوجيا والمعلومات.

تحليل النوعي للمخاطر: يتضمن تقييم الطبيعة والنوعية لكل مخاطرة وتحديد مدى تأثيرها.

تحليل الكمي للمخاطر: يشمل تقدير الاحتمالية والتأثير الكمي لكل مخاطرة.

وضع خطة الاستجابة للمخاطر: يجب وضع خطة تفصيلية لكيفية التعامل مع كل مخاطرة، بما في ذلك استراتيجيات التقليل من تأثيرها وإمكانية حدوثها.

تنفيذ خطة الاستجابة للمخاطر: يتضمن تنفيذ الإجراءات المحددة في خطة الاستجابة للمخاطر بشكل فعال وفعال.

باعتبار أن هذه الخطوات تعتمد على تحليل وتقييم الخطر التقني ووضع استراتيجيات للتعامل معه، يمكن

للمؤسسات تطبيق هذه الخطوات لتحقيق إدارة فعالة للمخاطر التقنية وضمان استمرارية العمل بشكل آمن وفعال.

المخاطر التقنية الشائعة في المصارف تشمل:

خطر الاختراق السيبراني والاختراقات الإلكترونية التي يمكن أن تتسبب في سرقة البيانات الحساسة والمالية.
خطر البرامج الضارة والفيروسات التي يمكن أن تعرض أنظمة المصارف للخطر وتسبب في فقدان البيانات.
خطر انقطاع الخدمات الإلكترونية مثل الخدمات المصرفية عبر الإنترنت، مما يؤثر على قدرة العملاء على الوصول إلى حساباتهم.

خطر تسرب البيانات وانتهاك الخصوصية، مما يمكن أن يؤدي إلى تعريض معلومات العملاء للخطر.
خطر عدم توفر الأمان السيبراني الكافي، مما يجعل المصارف عرضة للاختراقات والهجمات الإلكترونية.
هذه المخاطر تتطلب من المصارف تبني استراتيجيات قوية لإدارة المخاطر التقنية وتعزيز أمان البيانات والعمليات المصرفية الإلكترونية.

تعريف الأمان السيبراني:

يشير إلى عملية حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية والتهديدات السيبرانية. يعتمد الأمان السيبراني على تطبيق سياسات وإجراءات وتقنيات لحماية الأنظمة والمعلومات من الاختراقات والاعتداءات السلبية التي تستهدف سرقة المعلومات أو التسبب في تعطيل الخدمات الرقمية. (وزارة الاتصالات وتقنية المعلومات)

الأنواع الشائعة للهجمات السيبرانية في المصارف تشمل:

البرمجيات الخبيثة (Malware): وهي برامج تستخدم لاختراق الشبكات والأنظمة دون علم أصحابها، مما يتيح للمهاجمين سرقة البيانات المالية.
التصيد (Phishing): حيث يتم استخدام رسائل زور لخداع الأفراد والموظفين في المصارف للحصول على معلومات حساسة مثل بيانات الدخول.
حجب الخدمات (Denial Of Service): يهدف هذا النوع من الهجمات إلى تعطيل خدمات المصارف الإلكترونية، مما يؤدي إلى تعطيل الوصول للعملاء.

الهجمات دون انتظار (Zero-Day): تستغل هذه الهجمات ثغرات أمنية لم يتم اكتشافها مسبقًا، مما يتيح للمهاجمين الوصول غير المصرح به إلى الأنظمة المصرفية.

هذه الأنواع من الهجمات تشكل تحديًا كبيرًا للمصارف، مما يستدعي تبني استراتيجيات قوية للأمن السيبراني لحماية البيانات المالية وضمان استمرارية الخدمات المصرفية بشكل آمن. (تقرير المخاطر التي تواجه المصارف الإلكترونية قناة العربية).

أثر الهجمات السيبرانية القانونية و اقتصادية على المصارف:

تتضمن تأثيرات كبيرة على القطاع المصرفي. من الناحية القانونية، تتطلب هذه الهجمات استجابة قانونية فعالة لحماية البيانات وتحديد المسؤوليات عن الهجمات السيبرانية. من الناحية الاقتصادية، تتسبب الهجمات السيبرانية في خسائر مالية هائلة للمصارف، حيث يمكن أن تؤدي إلى تعطيل الخدمات المصرفية الإلكترونية، سرقة البيانات

المالية، وتقديم الخدمات المصرفية غير متاحة للعملاء. لذلك، يجب على المصارف تكثيف جهودها في تعزيز أمان البيانات وتطبيق استراتيجيات قوية لإدارة المخاطر التقنية بهدف حماية أنظمتها وبيانات عملائها.

لتدريب والتوعية بشأن الأمن السيبراني:

Microlearning التي توفر دورات تدريبية مجانية للتوعية بالأمن السيبراني

دورات تدريبية مخصصة تقدمها مؤسسات متخصصة في مجال الأمن السيبراني، مثل دفاع للأمن السيبراني التي تقدم دورات مخصصة لتدريب وزيادة الوعي في هذا المجال

برامج تدريبية داخلية مخصصة تُنفذ في الشركات والمؤسسات لتثقيف وتدريب الموظفين على مخاطر الأمن السيبراني وكيفية التصدي لها

الإطار التنظيمي للأمن السيبراني الذي يحدد المبادئ التوجيهية والتدابير الأساسية التي يجب اتباعها لضمان الأمان السيبراني في مؤسسات الاتصالات وتقنية المعلومات

هذه الأدوات تساهم في رفع مستوى الوعي وتزويد الأفراد والمؤسسات بالمعرفة والمهارات الضرورية لحماية أنظمتهم وبياناتهم من التهديدات السيبرانية.

لرصد الاختراقات التقنية، يمكن استخدام مجموعة متنوعة من الأدوات والتقنيات المتخصصة. بعض الأدوات والتقنيات المستخدمة تشمل:

برامج اكتشاف الاختراق : تساعد في تقييم قوة الأمان للأنظمة والتطبيقات من خلال محاكاة هجمات حقيقية لتحديد الثغرات والضعف في الأمان

أدوات مراقبة السلوك : تقوم بمراقبة السلوكيات غير المعتادة داخل النظام لاكتشاف أنشطة غير مرغوب فيها أو مشبوهة تشير إلى اختراق محتمل

أدوات تبادل التهديدات : توفر معلومات حول التهديدات السيبرانية الحالية والمستقبلية، مما يساعد في تحديد ومواجهة الاختراقات بشكل فعال

برامج مكافحة الفيروسات : تستخدم للكشف عن وإزالة البرامج الضارة والفيروسات التي قد تكون جزءًا من عمليات اختراق

هذه الأدوات والتقنيات تعمل سويًا لتوفير بيئة أمنية قوية ولرصد الاختراقات التقنية بشكل فعال لحماية الأنظمة والبيانات من التهديدات السيبرانية.

الفصل الثالث

الدراسات الدراسات السابقة

الدراسة الاولى

عنوان الدراسة:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم استقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

الهدف من الدراسة:

استعراض المدى الذي يمكن أن تساهم فيه جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الامن السيبراني في البنوك الإلكترونية وتأثير ذلك على دعم الاستقرار المالي.

إجراءات الدراسة:

استخدم الباحث المنهج الاستنباطي والاستقرائي المنهج الاستنباطي من خلال المسح لدراسات والبحوث بغية بناء إطار نظري للبحث والمنهج الاستقرائي في الدراسة الميدانية لجمع البيانات.

استنتاجات الدراسة

تعد الطبيعة المتطورة للأمن السيبراني غير قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بها يتم معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات.

الدراسة الثانية

عنوان الدراسة:

متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات إدارية بجامعة الملك سعود

الهدف من الدراسة:

معرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات إدارية بجامعة الملك سعود

إجراءات الدراسة:

يعتمد البحث على الاستبانة كأداة لجمع المعلومات من عينة من العاملين بالجامعة لتعرف على وجهة نظرهم.

استنتاجات الدراسة:

التأكيد على ضرورة اهتمام جامعة الملك سعود بمتطلبات حماية أنظمة المعلومات الادارية كما أشار إليها البحث وكما

أقر بها أفراد عينة البحث.

فروض البحث

هناك تأثير إيجابي عند اتباع أسس ونظام يرفع من مستوى الوقاية من المخاطر التقنية.

هناك علاقة بين مدى وعي العملاء بالمخاطر وإمكانية حدوثه.

هناك أثر سليم في حال التحقق من هوية المصدر في حال تلقى اي نوع من انواع التواصل.

الفصل الرابع

المنهجية وطرق البحث:

منهجية البحث:

تم استخدام المنهج الوصفي لتحليل ظواهر معينة وحالات تتعلق بالبحث أيضا تم استخدام المنهج الاستنباطي لاستخلاص استنتاجات من خلال تحليل البيانات المتاحة.

أدوات البحث:

تم اعتماد الملاحظة والاستبيان كأداة من أجل الحصول على المعلومات التي تلزم لاختبار الفرضيات من عينة من العملاء للمصارف في السعودية والبرمجيات المتخصصة في التحليل البياني.

مجالات الدراسة:

المجال المكاني

تم هذا البحث في جامعة ميداو شن برنامج ماجستير إدارة مخاطر

مجتمع الدراسة عينة من عملاء بعض المصارف السعودية

المجال الزمني

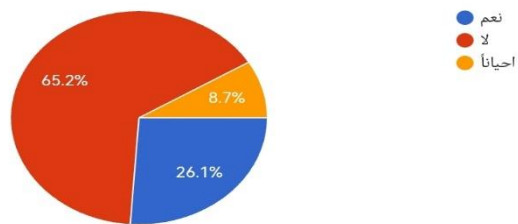
يتم إجراء الدراسة خلال الفصل الدراسي الثالث لعام 202٤

الفصل الخامس

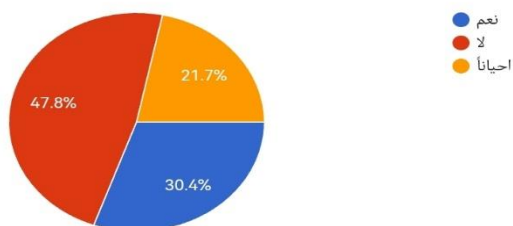
عرض ومناقشة نتائج الفرض الاول:

دى مشاركة البيانات الشخصية أو المالية على الإنترنت أو من خلال اتصال مجهول أيضا النقر العشوائي على الروابط المرسله من باب الفضول.

هل سبق وشاركت بيانات شخصية أو مالية على الإنترنت أو من خلال اتصال مجهول
23 ردًا



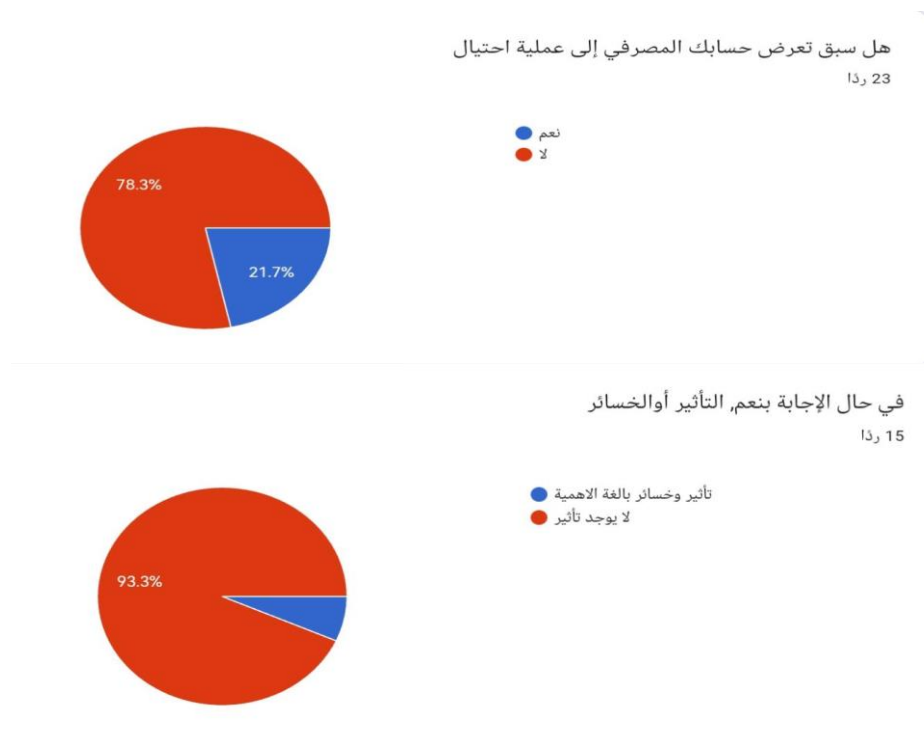
هل سبق ونقرت على رابط ارسل لك من باب الفضول دون علمك بالمحتوى
23 ردًا



في هذه الفرضية تشير النتائج على أن هناك تفاوت في مستوى الوعي لمخاطر تبادل البيانات الشخصية مع مجهول ولكن الغالبية العظمى لديها وعي إيجابي اتجاه هذا الخطر.

عرض ومناقشة نتائج الفرض الثاني:

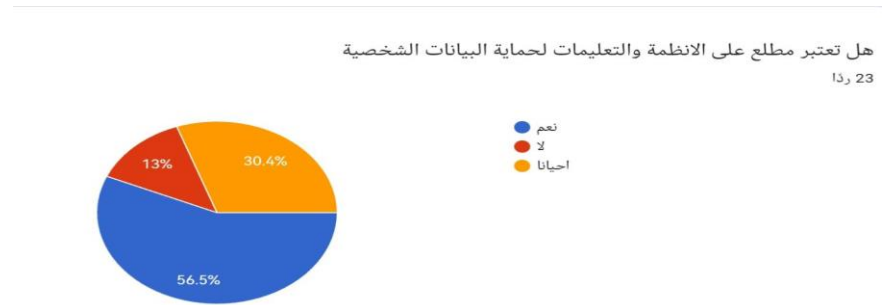
الخاص بمعدل تعرض بعض العملاء إلى عملية احتيال على حساباتهم المصرفية



تبعا للنتائج الظاهرة هناك نسبة قليل جدا تعرضت فعليا لعملية احتيال مصرفية وتأثرت منه بشكل بالغ الأهمية

عرض ومناقشة نتائج الفرض الثالث:

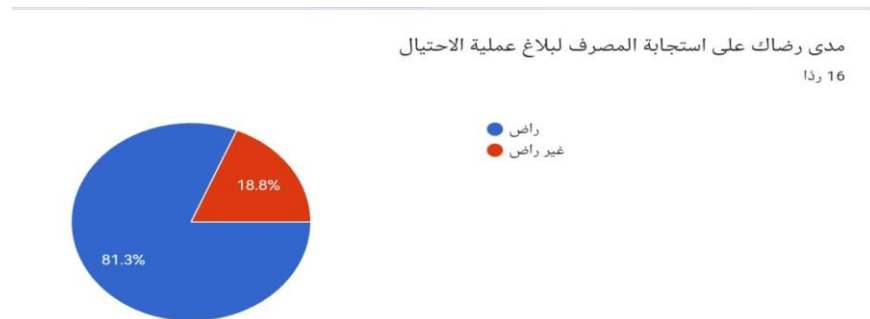
الخاص بنسبة الوعي وهل يعتقد العملاء أن الاختراقات التقنية بسبب ضعف الوعي بالأنظمة والقوانين ومدى اطلاعهم عليها.



في هذه الفرضية تناقض ما بين اعتقاد النسبة الأعلى من لعينه أن سبب الاختراقات التقنية لحساباتهم بسبب ضعف الوعي من قبل العملاء بينما هناك نسبة عالية جدا ذكرت بأنها مطلعة على

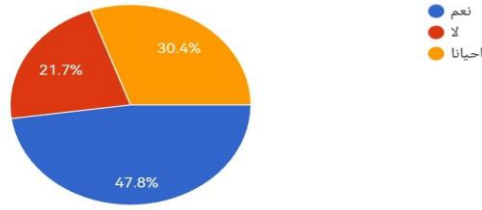
عرض ومناقشة نتائج الفرض الرابع:

مدى رضا العميل على الاستجابة لبلاغات الاحتيال وهل يعتقدون أن الاختراقات التقنية بسبب ضعف الأنظمة الإلكترونية للمصرف المستخدم.



هل تعتقد أن الاختراقات التقنية بسبب ضعف الأنظمة الإلكترونية للمصرف المستخدم

23 رداً



أيضاً هنا في هذه الفرضية تظهر نسبة عالية جداً راضية عن استجابة المصرف المستخدم لبلاغات الاحتيال بينما هناك قرابة نصف العينة ترجع سبب الاختراقات التقنية وعمليات الاحتيال إلى ضعف الأنظمة الإلكترونية للمصرف المستخدم من قبلهم.

الفصل السادس

الاستنتاجات :

التطورات السريعة في المخاطر التقنية على الأمن السيبراني في المصارف في السعودية تحفز المصارف على البحث المستمر والمكثف للوقاية من تلك المخاطر

يحتاج العملاء للمصارف توعية مستمرة حول مخاطر تبادل البيانات الشخصية المتعلقة بحساباتهم.

ضرورة التحقق من هوية المصدر قبل أي إجراء مثل إتمام الدفع الإلكتروني.

التوصيات:

وضع أسس واضحة لإدارة المخاطر التقنية على الأمن السيبراني في مجال المصارف في السعودية وتحديد المسؤوليات للجهات ذات العلاقة.

تكثيف الوعي بمخاطر تبادل البيانات الشخصية للحسابات المصرفية لدى العملاء للمصارف من خلال الرسائل النصية والاتصالات ذات الرد الآلي من حين لآخر .

التحقق من موثوقية المصدر في حال تلقى اتصال أو رابط إلكتروني و قبل إتمام عمليات الدفع الإلكتروني .

المصادر والمراجع:

المنصة الوطنية الموحدة GOV. SA

صحيفة الشرق الأوسط

بحث على بعنوان (إثر الأمن السيبراني على الأمن الوطني) جامعة عمان العربية 2022

دورة إدارة مخاطر منصة بكة

(تقرير المخاطر التي تواجه المصارف الإلكترونية قناة العربية).

موقع (وزارة الاتصالات وتقنية المعلومات)

ملخصات البحث

تم استخدام المنهج الوصفي لتحليل ظواهر معينة وحالات تتعلق بالبحث أيضا تم استخدام المنهج الاستنباطي لاستخلاص استنتاجات من خلال تحليل البيانات المتاحة.

تم اعتماد الملاحظة والاستبيان كأداة من أجل الحصول على المعلومات التي تلزم لاختبار الفرضيات من عينة من العملاء للمصارف في السعودية والبرمجيات المتخصصة في التحليل البياني.

تهدف الدراسة إلى التعرف على أثر تطبيق إدارة المخاطر التقنية للحد من الهجمات السيبرانية على أنظمة المصرفية في السعودية

The descriptive approach was used to analyze specific phenomena and cases related to research as well The deductive approach was used to draw conclusions by analyzing the .available data

The observation and questionnaire were adopted as a tool in order to obtain the information needed to test hypotheses from a sample of customers for banks in Saudi Arabia and software specialized in .graphic analysis

The study aims to identify the impact of the application of technical risk management to reduce cyber attacks on banking systems in Saudi Arabia



مستخلصات البحث:

ضرورة تبني اساس واضح لإدارة المخاطر التقنية على الأمن السيبراني للبنوك وتكثيف توعية العملاء بمخاطر عدم التحقق من هوية المصدر.

The need to adopt a clear basis for managing technical risks on the cybersecurity of banks and to intensify customer awareness of the risks of not verifying the identity of the issuer