Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. 74, Part (1): 677-689
Doi: www.doi.org/10.25130/tjaes.22.74.1.33

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

The impact of cybersecurity risks on banking services: An analytical study of a sample of banks operating in Iraqi Kurdistan

Yazen N. Mahmood*
Presidency/Ninevah University

Keywords:
Cybersecurity, Banking Services, Security Threats, Electronic Banking, Cyber Viruses.

A R T I C L E I N F O

Article history:

Received	29 Mar. 2026
Received in revised form	05 May. 2026
Accepted	05 May. 2026
Available online	30 Jun. 2026

*Corresponding author:
Yazen N. Mahmood
Presidency/Ninevah University

Abstract: In recent years, all banks have adopted the internet to provide their services to customers in the best possible way and at the highest possible level of quality. At the same time, banks have worked to prevent any external threats, especially those caused by viruses and malware on the web. This study aims to identify the level of security risks that banks deal with daily, such as Cihan Bank and Shirin Bank in Erbil, and how these security risks affect the nature of the electronic banking services provided by these banks to their customers. The research data was collected through a questionnaire distributed to employees of Cihan Bank and Shirin Bank. (112) questionnaires were distributed to the research sample, and (102) valid responses were obtained. The data from the questionnaires were collected and analyzed using SPSS software. The results indicated that phishing, Trojan horse viruses, and keyloggering programs have a significant impact on the security and efficiency of electronic banking services compared to database theft, which did not show a significant impact. Therefore, banks should continue to provide their employees with regular training on security threats and how to deal with them, given the constantly changing digital world. Furthermore, they should raise customer awareness of these risks and their impact on managing their accounts and transactions.

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. 74, Part (1): 677-689
Doi: www.doi.org/10.25130/tjaes.22.74.1.33

تأثير مخاطر الامن الالكتروني في الخدمات المصرفية: دراسة تحليلية لعينة من المصارف العاملة في كوردستان العراق

يزن نافع محمود
رئاسة الجامعة/جامعة نينوى

المستخلص

في السنوات الأخيرة اعتمدت جميع البنوك على الإنترنت لتقديم خدماتها للعملاء بأفضل الطرق وأعلى مستوى ممكن من الجودة، وفي الوقت نفسه عملت البنوك على منع أي تهديدات خارجية، خاصة تلك التي تسببها الفيروسات والبرمجيات الخبيثة الموجودة على شبكة الويب، إذ تهدف هذه الدراسة إلى التعرف على مستوى مخاطر الأمن التي تتعامل معها البنوك يومياً، كمصرف جيهان ومصرف شيرين في أربيل وكيف تؤثر هذه المخاطر الأمنية على طبيعة عمل خدمات الصيرفة الإلكترونية المقدمة من قبل هذه المصارف تجاه الزبائن.

إذ تم جمع بيانات البحث من خلال استبيان وُزّع على موظفي مصرف جيهان ومصرف شيرين، وقد تم توزيع (112) استبياناً على عينة البحث، وتم الحصول على (102) استجابة صالحة وجمعت البيانات من الاستبيان وتم تحليلها باستخدام برنامج (SPSS) وبعد إجراء التحليل تم التوصل إلى النتائج التي أشارت إلى أن التصيد الاحتيالي، وفيروسات حصان طروادة، وبرامج تسجيل لوحة المفاتيح لها تأثيرات معنوية على مستوى أمن وكفاءة الخدمات المصرفية الإلكترونية مقارنة بمتغير سرقة قاعدة البيانات الذي لم يظهر تأثير معنوي كبير وبناءً على ذلك يجب على البنوك الاستمرار في تدريب موظفيها بشكل دوري حول التهديدات الأمنية وطرق التعامل معها كونها في عالم رقمي متغير باستمرار فضلا عن زيادة وعي العملاء حل هذه المخاطر تأثيرها على ادارة حساباتهم وتعاملاتهم.

الكلمات المفتاحية: الأمن الالكتروني، الخدمات المصرفية، التهديدات الأمنية، الصيرفة الالكترونية، الفيرسات الالكترونية

المقدمة

في السنوات الأخيرة أدى التطور السريع في تكنولوجيا المعلومات والانتشار الواسع لاستخدام الإنترنت إلى إحداث تغييرات كبيرة في القطاع المصرفي. فقد اتجهت البنوك بشكل متزايد إلى اعتماد خدمات الصيرفة الإلكترونية (E-Banking) لتقديم خدمات أسرع وأكثر سهولة وكفاءة لعملائها. ومن خلال الصيرفة الإلكترونية يمكن للعملاء إجراء العديد من المعاملات المالية مثل تحويل الأموال، والتحقق من أرصدة الحسابات، ودفع الفواتير دون الحاجة إلى زيارة فروع البنك.

ومع ذلك، فأن الاعتماد المتزايد على الأنظمة المصرفية المعتمدة على الإنترنت أدى أيضاً إلى ظهور العديد من المخاطر الأمنية. فالهجمات الإلكترونية مثل الفيروسات، والاختراقات، والتصيد الاحتيالي، وتسريب البيانات يمكن أن تهدد سرية المعلومات المصرفية وسلامتها وتوفرها. لذلك أصبحت مسألة الأمن من أهم القضايا التي يجب على البنوك الاهتمام بها لحماية أنظمتها والحفاظ على ثقة عملائها.

لذلك فأن فهم وقياس المخاطر الأمنية في أنظمة الصيرفة الإلكترونية يعد أمراً ضرورياً للبنوك، خاصة في البيئات المالية النامية. وتركز هذه الدراسة على تحديد وتقييم المخاطر الأمنية التي

تواجه البنوك في إقليم كوردستان العراق، فضلا عن دراسة تأثير هذه المخاطر على جودة وموثوقية خدمات الصيرفة الإلكترونية.

المبحث الأول: الدراسات السابقة ومنهجية البحث

المحور الأول: الدراسات السابقة

ت	الباحث	البحث	الوصف
1	Waliullah, M.& Others2025	Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review	يشير هذا البحث الى أكثر التهديدات السيبرانية شيوعًا التي تستهدف منصات الخدمات المصرفية الرقمية، وفعالية التدابير الأمنية الحديثة، ودور الأطر التنظيمية في الحد من مخاطر الأمن السيبراني المالي. واشارت النتائج إلى أن هجمات التصيد الاحتيالي والبرمجيات الخبيثة لا تزال أكثر التهديدات السيبرانية شيوعًا، مما يؤدي إلى خسائر مالية فادحة وفقدان ثقة المستهلكين، ومع توفر تقنيات كشف الاحتيال المدعومة بالذكاء الاصطناعي وفرت حلولاً واعدة لتأمين المعاملات المالية.
2	Gabriela Mogos1& Others, 2021	Study on security risks of e-banking system	يهدف هذا البحث إلى تحديد الوضع الأمني لتطبيق الخدمات المصرفية الإلكترونية وتحليل المخاطر والهجمات التي قد يتعرض لها العملاء. وقد ذُكرت عدة إجراءات للتخفيف من هذه الهجمات، مثل التحكم في الوصول للحد من التنصت، وهذا يعني أن تقييد الوصول إلى البيانات الحساسة إلزامي. ويُظهر هذا البحث كيفية تطبيق العديد من تدابير الحماية المختلفة لحماية الفرد والمنظمة من أن يصبح هدفًا للجرائم الإلكترونية.
3	Rami Shehab & Others,2024	Assessment of Cybersecurity Risks and threats on Banking and Financial Services	يصف هذا البحث أهم التهديدات والتحديات التي يجب مراعاتها عند التعامل مع البنوك والمؤسسات المالية ونقاط الضعف في البنية التحتية للبنوك والمؤسسات المالية، والتي تُؤدي إلى تصاعد الهجمات على القطاع وتؤثر على النظام المصرفي والأفراد والمنظمات وقد تبين أن هجمات البرامج الضارة هي أكثر التهديدات شيوعًا للبنوك والمؤسسات المالية. يُعد تبادل المعلومات بين البنوك والمؤسسات المالية،

المحور الثاني: منهجية البحث

أولاً. مشكلة البحث :يهدف هذا البحث إلى معرفة تأثير المخاطر الأمنية على الخدمات الصيرفة الإلكترونية في المصارف العاملة في إقليم كوردستان العراق وخصوصا أن البيئة الرقمية تشهد تطورا سريعا في المجال الرقمي ومعه تزداد المخاطر والتحديات صعوبة، ومعرفة طبيعة تأثير هذه المخاطر والتحديات المتواجدة في البيئة الرقمية المتغيرة باستمرار على طبيعة عمل البنوك في الاقليم بما تمتلكه من الامكانيات المحدودة مقارنة مع البنوك العالمية، وعليه فأن مشكلة البحث تتمثل في السؤال الآتي:

- كيف تؤثر المخاطر الأمنية على خدمات الصيرفة الإلكترونية التي تقدمها المصارف للزبائن في العصر التقني الحالي؟

ثانياً. أهمية البحث:

1. دراسة طبيعة خدمات الصيرفة الإلكترونية التي تقدمها هذه مصارف الأهلية (مصرف جيهان ومصرف شيرين) وكيفية تعامل هذه المصارف مع المشكلات وما هي التحديات الأكثر تأثيرا عليها في مجال التهديدات والمخاطر الأمنية لتي تتعامل معها يوميا.
2. تتمثل بالإجابة عن الفرضيات التي تمت صياغتها في البحث وحل المشكلة التي تم اقتراحها في البحث فضلا عن تقديم العديد من التوصيات التي يجب العمل بها مستقبلا.
3. تقديم خلفية نظرية عن خدمات الصيرفة الإلكترونية في المقدمة من قبل المصارف الأهلية العاملة في القطاع المصرفي وطبيعة التهديدات الأمنية والتحديات التي تواجهها تلك المصارف في التعامل معها.

ثالثاً. أهداف البحث:

1. التعرف على مدى انتشار التهديدات الامنية في خدمات الصيرفة في الميدان الخاص بهذه الدراسة.
2. معرفة تأثير كل متغير من متغيرات المخاطر الأمنية على الخدمات الصيرفة الالكترونية.
3. اختبار العلاقة بين المخاطر الامنية وخدمات الصيرفة الالكترونية.
4. اعطاء جانب عملي يساعد على فهم طبيعة العلاقة بين المتغيرات المذكورة لأجل اعتماده في دراسات مستقبلية.

رابعاً. فرضيات البحث: استناداً إلى مشكلة البحث وأهميته، حددت الدراسة الفرضيات الأساسية كما يأتي:

H0: تؤثر مخاطر التهديدات الأمنية على خدمات الصيرفة الإلكترونية.

ومن هذه الفرضية تنبثق الفرضيات الفرعية الآتية:

H1: يؤثر تهديد التصيد الاحتيالي (Phishing) على خدمات الصيرفة الإلكترونية.

H2: يؤثر تهديد سرقة قاعدة بيانات كلمات المرور (Password Database Theft) على خدمات الصيرفة الإلكترونية.

H3: يؤثر تهديد فيروس حصان طروادة (Trojan Virus) على خدمات الصيرفة الإلكترونية.

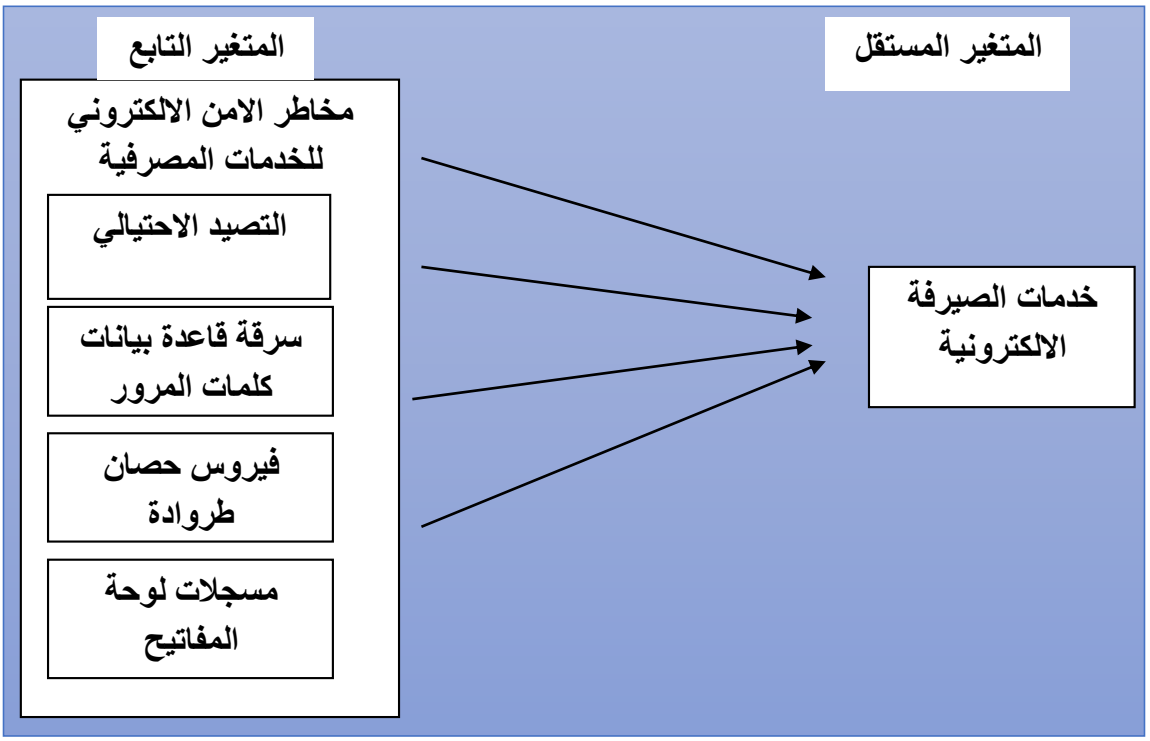
H4: يؤثر تهديد مسجلات لوحة المفاتيح (Keyloggers) على خدمات الصيرفة الإلكترونية.

خامساً. ادوات البحث: اعتمد هذا البحث على المنهج الوصفي التحليلي لأجل اختبار الفرضيات التي تم اعتمادها من خلال بيان علاقات الأثر والارتباط من خلال اعتماد استمارة استبيان تم توزيعها على عينة البحث (مصرف جيهان ومصرف شيرين) والتي اعتمدت على المقياس الخامسي لليكرت،

وبالاعتماد على الادوات والبرامج الاحصائية والتي تمثلت ببرنامج (SPSS) في اجراء التحليلات الرياضية والاحصائية التي تمت في هذا البحث.

سادسا. مجتمع وعينة الدراسة: تألف مجتمع الدراسة من عينة من الأفراد في مصرف جيهان ومصرف شيرين والبالغ عددهم حوال (112) عينة قد تم الحصول على (102) عينة صالحة لأجل التحليل الاحصائي.

سابعا: مخطط الدراسة



المبحث الثاني: الإطار النظري

أولاً. الخلفية التاريخية للخدمات الإلكترونية (E-Banking): شهد قطاع الخدمات المالية الإلكترونية تطورات كبيرة خلال السنوات الأخيرة الماضية. ‘إذ اعتمدت البنوك سابقا بشكل كبير على الفروع التقليدية لتقديم الخدمات المالية، ولم يكن هناك ضغط كبير لإحداث تغييرات في طرق تقديم الخدمات. لكن هذا الوضع بدأ يتغير تدريجياً مع تحرير القطاع المالي حيث أدى التطور المتزايد في تكنولوجيا المعلومات والاتصالات إلى زيادة المنافسة وفرض وتيرة أسرع للتغيير (Kara, 2021: 11).

ويُعد الإنترنت قناة حديثة نسبياً لتقديم الخدمات المصرفية. فقد ظهرت أولى أشكال الخدمات المصرفية عبر الإنترنت في بداية الثمانينيات تحت مسمى الخدمات المصرفية عبر الحاسوب (Online Banking)، والتي كانت تتطلب وجود حاسوب شخصي ومودم وبرمجيات خاصة توفرها المؤسسات المالية. إلا أن هذه الخدمات لم تلقَ قبولاً واسعاً في البداية، وتم إيقاف معظم المبادرات المرتبطة بها. ومع النمو السريع لأنواع أخرى من الخدمات الإلكترونية منذ منتصف التسعينيات، عادت البنوك للاهتمام بوسائل تقديم الخدمات الإلكترونية عبر الإنترنت (Safi & Singh, 2023: 9).

ثانياً. تعريف الصيرفة الإلكترونية (E-Banking): يتم تعريف الصيرفة الإلكترونية على أنها تقديم المنتجات والخدمات المصرفية للأفراد والشركات ذات القيم الصغيرة من خلال القنوات الإلكترونية، فضلا عن عمليات الدفع الإلكترونية ذات القيم الكبيرة والخدمات المصرفية بالجملة التي يتم تقديمها إلكترونيا (Riasat & Gonul, 2025: 13)

وأشار (Căciulescu, & Others, 2024: 17) إليها على أنها التحويل الإلكتروني للأموال مباشرة من حساب إلى آخر بدلاً من استخدام الشيكات أو النقود. ووفقاً لـ (Adekoya & Others,. 2025: 3) فأن البنك تُعرف الصيرفة الإلكترونية بأنها مصطلح شامل يشير إلى العملية التي يستطيع من خلالها العميل إجراء معاملاته المصرفية إلكترونياً دون الحاجة إلى زيارة المؤسسة المصرفية التقليدية

ثالثا. أنواع خدمات الصيرفة الإلكترونية: وفقاً لكل من (Tn & Kulkarni, 2023: 21) و(Kyaw, & Others, 2024: 19) و(Ahmad & Iqbal, 2024: 4) و (Bongiovanni & Others, 2023: 10) توجد عدة أنواع من خدمات الصيرفة الإلكترونية، من أهمها:

1. الخدمات المصرفية المنزلية (Home Banking): تتيح للعملاء الحصول على معلومات حول حساباتهم الشخصية باستخدام كلمات المرور والرموز الخاصة للدخول إلى البيانات، كما يمكنهم إجراء تحويلات مالية من حساب إلى آخر عبر الاتصال الهاتفي.
2. الخدمات المصرفية عبر الحاسوب (PC Banking): وهي نوع من الخدمات المصرفية التي تمكّن العملاء من تنفيذ المعاملات المصرفية من خلال جهاز الحاسوب باستخدام برنامج مالي خاص توفره المؤسسة المصرفية.
3. الخدمات المصرفية عبر الإنترنت (Internet Banking): وتعرف أيضاً باسم الخدمات المصرفية عبر الويب أو الخدمات المصرفية الافتراضية، وهي نظام يسمح للعملاء بالوصول إلى حساباتهم ومعلومات المنتجات والخدمات المصرفية مباشرة من خلال الحاسوب الشخصي باستخدام الإنترنت.
4. الخدمات المصرفية عبر الهاتف المحمول (Mobile Banking): وهي نظام يتيح لعملاء البنوك إجراء معاملات مالية مختلفة باستخدام الأجهزة المحمولة، وتُعد من أحدث خدمات الصيرفة الإلكترونية، وتعتمد على بروتوكول التطبيقات اللاسلكية.(WAP)

وفقاً لـ (Uddin &Others ,2023,31)توجد خدمات أخرى للصيرفة الإلكترونية، من أهمها:

أ. الصراف الآلي (Automatic Teller Machine-ATM): جهاز الصراف الآلي هو جهاز إلكتروني محوسب للاتصالات يسمح للعملاء باستخدام تكنولوجيا المعلومات للوصول مباشرة إلى حساباتهم المصرفية والتحقق من أرصدتهم دون الحاجة إلى وجود موظف في البنك.

ولاستخدام هذه الخدمة، يحتاج العميل إلى فتح حساب مصرفي في البنك وإيداع الأموال فيه، وبعد ذلك يقوم البنك بإعطائه بطاقة خاصة تسمى بطاقة الصراف الآلي (ATM Card) مع رقم تعريف شخصي .(PIN) ومن خلال هذه البطاقة يمكن للعميل سحب الأموال من أي جهاز صراف آلي تابع للبنك (Uddin & Others, 2020: 7).

ب.الشيك الإلكتروني (E-Cheque): يتمتع الشيك الإلكتروني بجميع خصائص الشيك الورقي التقليدي، ويمكن استخدامه في أنواع مختلفة من المدفوعات مثل المدفوعات المشروطة أو المسماة أو الحكومية أو غير النقدية (Aldasoro & Others, 2020: 12).

ويتضمن الشيك الإلكتروني مجموعة من الحقول المهمة مثل: رقم الشيك، ومفتاح التشفير، وبيانات الحساب البنكي للدافع، وبيانات الحساب البنكي للمستفيد، وقيمة المبلغ، وتاريخ الدفع، فضلا عن نوع الشيك وحدوده وإجراءات معالجته. وتختلف طرق تصميم حقول الشيك الإلكتروني تبعاً للقوانين والأنظمة المعتمدة في كل دولة (Smaga, 2025,8).

رابعاً. التهديدات الأمنية في الصيرفة الإلكترونية: أصبح أمن الصيرفة الإلكترونية خلال العقد الأخير من أهم القضايا في قطاع الخدمات المالية، إذ توجد العديد من التهديدات التي يمكن أن تؤثر على خدمات الصيرفة الإلكترونية، ووفقاً لـ (Thomopoulos & Others, 2024: 32) و (Pollmeier & ,2023; 26) و(Bruce & Others, 2024: 3) و(Bajwa & Others, 2023: 29) توجد العديد من التهديدات على الإنترنت التي يمكن أن تؤثر على خدمات الصيرفة الإلكترونية، ومن أهمها:

1. **التصيد الاحتيالي (Phishing):** يُعد التصيد الاحتيالي أحد أشكال الجرائم الإلكترونية الشائعة على الإنترنت. ويتم تنفيذه غالباً عبر وسائل التواصل الاجتماعي مثل Facebookأو من خلال تطبيقات أو مواقع مزيفة أو رسائل بريد إلكتروني تطلب من المستخدم إرسال معلومات شخصية مثل اسم المستخدم وكلمة المرور وأرقام الضمان الاجتماعي أو بيانات البطاقات المصرفية.

كما يمكن أن يستهدف التصيد الاحتيالي خدمات الصيرفة الإلكترونية مثل أجهزة الصراف الآلي بطريقتين:

احتيال البطاقات :(Card Trapping) يتم سرقة بطاقة العميل عند إدخالها في جهاز الصراف الآلي من خلال وضع أداة داخل قارئ البطاقة تمنع خروجها بعد انتهاء العملية.

احتيال الأموال :(Currency Trapping) يتم وضع شريط لاصق داخل فتحة خروج النقود لمنع خروج الأموال وسرقتها لاحقاً.

2. **سرقة قاعدة بيانات كلمات المرور (Password Database Theft):** تُعد معلومات العملاء ذات قيمة كبيرة بالنسبة للقراصنة، لذلك يحاولون الحصول على بيانات الدخول للحسابات المصرفية بطرق مختلفة مثل سرقة بيانات الاعتماد أو إنشاء مواقع إلكترونية مزيفة. وبعد الحصول على البيانات قد يستخدمونها للابتزاز أو سرقة الأموال من الحسابات المصرفية.

ومن أشهر الأساليب المستخدمة في ذلك:

انتحال الهوية :(Spoofing) من خلال إنشاء مواقع مزيفة تشبه المواقع الأصلية للخدمات المصرفية عبر الإنترنت.

التصيد الصوتي :(Vishing) وهو مزيج من الاتصال الصوتي والتصيد الاحتيالي باستخدام تقنية VoIPللحصول على المعلومات المالية عبر الهاتف.

3. **فيروس حصان طروادة (Trojan Virus):** يعتمد هذا النوع من الهجمات على طريقتين رئيستين:

أ. هجوم الرجل في الوسط (Man-in-the-Middle-MitM): ومن أنواعه ما يعرف بـ (Pharming)، إذ يتم إدخال برنامج خبيث في رسالة أو تطبيق أو بريد إلكتروني. وعند فتح الرسالة يتمكن الفيروس من السيطرة على جهاز المستخدم أو حسابه.

ب.بهجوم الرجل في المتصفح (Man-in-the-Browser – MitB): وهو برنامج حصان طروادة قادر على تعديل المعاملات المصرفية أو اعتراضها وتحويلها إلى حساب آخر. ومن أمثلة ذلك برنامج Silent Banker

4. **مسجلات لوحة المفاتيح (Keyloggers):** هي برامج خبيثة يتم تثبيتها على جهاز الحاسوب الخاص بالمستخدم، وتقوم بتسجيل كل ضغطة على لوحة المفاتيح عند دخول المستخدم إلى موقع البنك. وبذلك يستطيع المخترق الحصول على بيانات تسجيل الدخول الخاصة بالعميل والسيطرة على حسابه المصرفي

خامساً. قواعد الأمان للحماية في الصيرفة الإلكترونية: حدّد (Birindelli& Iannuzzi, 2024: 18) و (Türegün, 2025: 16) و(Jin & Others, 2023: 5) مجموعة قواعد مهمة للحفاظ على أمن الحاسوب والمعلومات من التهديدات والفيروسات، وهي:

1. تثبيت برامج الحماية: تصبح المعلومات معرضة للخطر عند الاتصال بالإنترنت، لذلك يجب تثبيت برامج الحماية مثل جدار الحماية (Firewall) لمنع سرقة المعلومات.
2. حماية البيانات الحساسة عند إرسالها عبر الشبكات المفتوحة: يجب تشفير المعلومات قبل إرسالها لتجنب اعتراضها أثناء النقل.
3. معرفة الجهة التي ستستلم المعلومات: يجب التأكد من صحة البريد الإلكتروني أو الموقع الإلكتروني لتجنب المواقع المزيفة.
4. عدم تخزين البيانات الحساسة: مثل كلمات المرور أو أرقام التعريف الشخصية أو بيانات بطاقات الائتمان.
5. اختيار كلمة مرور قوية: باستخدام مزيج من الحروف والأرقام والرموز وعدم استخدام معلومات شخصية مثل تاريخ الميلاد.
6. استخدام برامج حماية موثوقة فقط: لأن بعض البرامج الموجودة على الإنترنت قد تكون مزيفة أو تحتوي على فيروسات.
7. تحديث البرامج باستمرار: حيث تقوم الشركات بإضافة تحديثات أمنية تعرف باسم Patches أو Bug Fixesلتحسين مستوى الحماية.
8. إجراء فحص أمني للحاسوب: قبل الاتصال بالحساب المصرفي عبر الإنترنت.
9. تفعيل إعدادات الأمان في المتصفح: لأن ذلك يساعد في زيادة حماية المعلومات أثناء تصفح الإنترنت.
10. عدم إتاحة الحساب للآخرين: من خلال عدم مشاركة كلمة المرور مع أي شخص وعدم استخدام كلمات مرور سهلة التخمين.

المبحث الثالث: الدراسة التطبيقية

في هذا المبحث تم التطرق للجانب العملي من البحث وشمل بيانات عينة البحث فضلا عن القيام باختبارات عدة تضمنت اختبار الثبات واختبار تحليل الانحدار والارتباط.

أولاً. جمع البيانات وتحليلها:

جدول (1): البيانات الديموغرافية لعينة البحث

العوامل	الفئة	النسبة المئوية
الجنس	ذكر	69%
	أنثى	31%
العمر	أقل من 25 سنة	3%
	(26 – 35) سنة	47%

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. 74, Part (1): 677-689
Doi: www.doi.org/10.25130/tjaes.22.74.1.33

العوامل	الفئة	النسبة المئوية
	(36 – 46)سنة	39%
	أكثر من 46 سنة	11%
المستوى التعليمي	دبلوم	4%
	بكالوريوس	89%
	ماجستير	%6
	دكتوراه	%1

المصدر: إعداد الباحث.

تشير البيانات الديموغرافية إلى أن غالبية المشاركين في الدراسة من الذكور بنسبة 69%، بينما بلغت نسبة الإناث 31%كما يتضح أن الفئة العمرية الأكثر تمثيلاً في العينة هي 26–35سنة بنسبة 47%، تليها الفئة العمرية 36–46سنة بنسبة 39%أما من حيث المستوى التعليمي، فقد كان معظم المشاركين من حملة درجة البكالوريوس بنسبة 89%، وهو ما يدل على أن غالبية العاملين في البنوك يتمتعون بمستوى تعليمي جيد يؤهلهم لفهم واستخدام تقنيات الصيرفة الإلكترونية.

ثانياً. اختبار الثبات كرونباخ الفا (Cronbach's Alpha): أجرى الباحث اختبار الثبات للتحقق من ملاءمة المقاييس وقياس الاتساق الداخلي بين الفقرات من خلال معيار الاختبار كرونباخ الفا. حيث كلما اقتربت قيمة كرونباخ من 1 دل ذلك على زيادة موثوقية القياس كما وتعتبر قيمة كرونباخ 0.7 فأكثر مقبولة وتعد القيمة الأقل من 0.7 وأكثر من 0.6 ذات اتساق داخلي ضعيف أما إذا كانت القيمة أقل من 0.6 فلا يوجد اتساق داخلي بين المقاييس. الجدول رقم (2) أدناه يبين نتائج اختبار الثبات للقياسات.

جدول (2): اختبار الثبات

المقياس	عدد الفقرات	كرونباخ الفا (Cronbach's Alpha)	الحالة
التصيد الاحتيالي	5	0.851	مقبولة
سرقة قاعدة بيانات كلمات المرور	5	0.788	مقبولة
فيروس حصان طروادة	5	0.812	مقبولة
مسجلات لوحة المفاتيح	5	0.732	مقبولة
الصيرفة الإلكترونية	7	0.898	مقبولة

ثالثاً. تحليل الانحدار المتعدد (Multiple Regression): يلخص الجدول الآتي نتائج تحليل الانحدار:

جدول (3): نتائج تحليل الانحدار

المؤشر	القيمة
R Square	0.616
القيمة المعنوية(Significance)	0.041

المصدر :إعداد الباحث بالاعتماد على نتائج SPSS

من أجل التحقق من مدى تأثير المخاطر الامنية على الخدمات الصيرفة الالكترونية، تم استخدام تحليل الانحدار المتعدد .تشير قيمة $R^2 = 0.616$ إلى أن حوالي 60% من التباين في المتغير خدمات الصيرفة الإلكترونية يمكن تفسيره من خلال المتغيرات المتعلقة بالتهديدات الأمنية. كما أن القيمة المعنوية 0.041 أقل من 0.05، مما يدل على وجود علاقة ذات دلالة إحصائية بين المتغيرات، ومن ثم يتم دعم الفرضية الأولى .وهذا يعني أن التغير في المتغيرات المستقلة يفسر نسبة كبيرة من التغير في المتغير التابع.

رابعاً. تحليل الارتباط:

جدول (4): نتائج تحليل الارتباط

المتغير التابع	المتغير المستقل
عوامل التهديد الأمني	0.519*

N =102 $p < 0.05$

المصدر :إعداد الباحث.

يوضح تحليل الارتباط وجود علاقة إيجابية ذات دلالة إحصائية بين التهديدات الأمنية وخدمات الصيرفة الإلكترونية، إذ بلغت قيمة معامل الارتباط 0.519، وهي قيمة تشير إلى علاقة متوسطة القوة. وهذا يدل على أن زيادة التهديدات الأمنية قد تؤثر بشكل مباشر على كفاءة وأمان خدمات الصيرفة الإلكترونية.

خامساً. معاملات الانحدار:

جدول (5): معاملات الانحدار

المتغير المستقل	Beta	P
التصيد الاحتيالي	0.266	0.049*
فيروس حصان طروادة	0.186	0.036*
سرقة قاعدة بيانات كلمات المرور	0.015	(0.051 غير معنوي)
مسجلات لوحة المفاتيح	0.371	0.044*

* $P < 0.05$

المصدر إعداد الباحث.

تشير نتائج معاملات الانحدار إلى ما يأتي:

- التصيد الاحتيالي (Phishing): بلغت قيمة Beta 0.266 وهي قيمة موجبة ومعنوية، مما يدل على أن التصيد الاحتيالي يؤثر بشكل ملحوظ على خدمات الصيرفة الإلكترونية، بمعنى آخر أن التصيد الاحتيالي له تأثير معنوي وموجب على الخدمات المصرفية وبالتالي تُقبل الفرضية الأولى.
- فيروس حصان طروادة (Trojan Virus): بلغت قيمة Beta 0.186 وهي أيضاً موجبة ومعنوية، مما يشير إلى أن هذا النوع من الفيروسات يشكل تهديداً حقيقياً لأنظمة الصيرفة الإلكترونية، بمعنى وجود تأثير معنوي لكنه أضعف من تأثير التصيد الاحتيالي وبالتالي تُقبل الفرضية الثانية.
- سرقة قاعدة بيانات كلمات المرور (Password Database Theft): بلغت قيمة Beta 0.015 وهي غير معنوية، مما يدل على أن هذا العامل لم يظهر تأثيراً واضحاً في هذه الدراسة، أي لا يوجد تأثير معنوي لسرقة قاعدة بيانات كلمة المرور على الخدمات المصرفية ومن ثم لا تُقبل الفرضية الثالثة.

❖ مسجلات لوحة المفاتيح (Keyloggers): بلغت قيمة Beta 0.371 وهي أعلى قيمة بين المتغيرات، كما أنها موجبة ومعنوية، مما يدل على أن هذا التهديد له أقوى تأثير على خدمات الصيرفة الإلكترونية، ومن ثم تُقبل الفرضية الرابعة.

المبحث الرابع: الاستنتاجات والتوصيات

أولاً. الاستنتاجات:

1. كما أظهرت النتائج أن مسجلات لوحة المفاتيح تعد من أكثر التهديدات تأثيراً، لأنها قادرة على سرقة بيانات تسجيل الدخول الخاصة بالمستخدمين بسهولة دون علمهم. أما التصيد الاحتيالي فيعد من التهديدات الشائعة التي تعتمد على خداع المستخدمين للحصول على معلوماتهم الشخصية والمالية.
2. أشارت الدراسة إلى أن التهديدات الأمنية تلعب دوراً مهماً في التأثير على خدمات الصيرفة الإلكترونية في البنوك. فقد أظهرت النتائج أن التصيد الاحتيالي، وفيروسات حصان طروادة، وبرامج تسجيل لوحة المفاتيح لها تأثيرات معنوية على مستوى أمن وكفاءة الخدمات المصرفية الإلكترونية.
3. من ناحية أخرى، لم يظهر تهديد سرقة قاعدة بيانات كلمات المرور تأثيراً معنوياً في هذه الدراسة، وقد يرجع ذلك إلى اعتماد البنوك على أنظمة حماية متقدمة وقواعد بيانات مؤمنة تقلل من احتمالية حدوث هذا النوع من الهجمات فضلا عن محدودية الاشخاص الذين يمتلكون الصلاحية والمخولين في الدخول إلى الأنظمة.
4. بينت الدراسة أن موظفي البنوك لديهم معرفة جيدة بكيفية التعامل مع هذه المخاطر، خاصة مع تهديد مسجلات لوحة المفاتيح الذي يعد من التهديدات المنتشرة حالياً على شبكة الإنترنت العالمية (WWW)، كما يمتلك الموظفون القدرة على إيجاد حلول مناسبة لتجنب هذه المخاطر.
5. بشكل عام، تؤكد هذه النتائج أهمية تعزيز أنظمة الأمن في البنوك، وزيادة وعي الموظفين والعملاء بالمخاطر الإلكترونية، فضلا عن استخدام تقنيات الحماية المتقدمة مثل التشفير، والمصادقة متعددة العوامل، وأنظمة كشف الاختراق، وذلك لضمان تقديم خدمات مصرفية إلكترونية آمنة وموثوقة.

ثانياً. التوصيات:

1. ينبغي على البنوك الاستمرار في تدريب موظفيها بشكل دوري حول التهديدات الأمنية وطرق التعامل معها، بالإضافة إلى تعريفهم بأي تهديدات جديدة قد تظهر في المستقبل.
2. يجب زيادة وعي العملاء بالمخاطر الأمنية المرتبطة بالصيرفة الإلكترونية، وتشجيعهم على استخدام كلمات مرور قوية والحفاظ على سرية معلوماتهم المصرفية.
3. من الضروري أن تقوم البنوك بتنظيم دورات تدريبية وتوعوية للموظفين الجدد والعملاء حول مخاطر الأمن السيبراني وطرق الحماية من التهديدات الإلكترونية.

المصادر

1. Adekoya, O. A., Atlam, H. F., & Lallie, H. S. (2025). Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. Sensors, 25(14), 4345.
2. Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. Journal of Financial Crime, 31(6), 1485-1501.
3. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector.

4. Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. Information & computer security, 31(5), 635-654.
5. Birindelli, G., & Iannuzzi, A. P. (2024). The systemic importance of cyber risk in banks. In Systemic risk and complex networks in modern financial systems (pp. 301-321). Cham: Springer Nature Switzerland.
6. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one, 19(4), e0297312.
7. Căciulescu, A. R., Rughiniș, R., Țurcanu, D., & Radovici, A. (2024). Mapping cyber-financial risk profiles: Implications for european cybersecurity and financial literacy. Risks, 12(12), 200.
8. Jin, J., Li, N., Liu, S., & Nainar, S. K. (2023). Cyber attacks, discretionary loan loss provisions, and banks' earnings management. Finance Research Letters, 54, 103705.
9. Kara, I. (2021). Don't bite the bait: phishing attack for internet banking (e-banking). The Journal of Digital Forensics, Security and Law: JDFSL, 16, 1-12.
10. Kyaw, P. H., Gutierrez, J., & Ghobakhlou, A. (2024). A systematic review of deep learning techniques for phishing email detection. Electronics, 13(19), 3823.
11. Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 159, 106022.
12. Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening Cybersecurity Resilience: An Investigation of Customers Adoption of Emerging Security Tools in Mobile Banking Apps. Computers, 14 (4), 129.
13. Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. Journal of King Saud University-Computer and Information Sciences, 35(2), 590-611.
14. Smaga, P. (2025). Profiling the victim-cyber risk in commercial banks. Computers & Security, 150, 104274.
15. Thomopoulos, G. A., Lyras, D. P., & Fidas, C. A. (2024). A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective. Personal and Ubiquitous Computing, 28(3), 449-470.
16. Tn, N., & Shailendra Kulkarni, M. (2023). Zero click attacks–a new cyber threat for the e-banking sector. Journal of Financial Crime, 30(5), 1150-1161.
17. Türegün, N. (2025). Digital transformation and cybersecurity risks. International Journal of Accounting Information Systems, 56, 100749.
18. Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability?. International Review of Financial Analysis, 72, 101587.
19. Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure?. Technological Forecasting and Social Change, 197, 122919.
20. Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the

adoption and growth of digital banking: a systematic literature review. arXiv preprint arXiv:2503.22710

21. Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. Indonesian Journal of Electrical Engineering and Computer Science, 21(2), 1065-1072
22. Shehab, R., Al-Abed, M., & Al-Shargabi, B. (2024). Assessment of cybersecurity risks and threats on banking and financial institutions. Journal of Information Systems and Informatics Security (JISIS), 3(3).