مجلة البحوث الأكاديمية

Journal homepage: www.lam.edu.ly

تقييم الوعي بأمن المعلومات لدى العاملين في القطاع المصرفي الخاص في مصراتة – ليبيا

علي عبد الحفيظ الروياتي
قسم الهندسة الإلكترونية– كلية التقنية الصناعية – مصراتة
elrowayati@yahoo.com

سراج الدين مصطفى السويدي
قسم الهندسة الإلكترونية– كلية التقنية الصناعية – مصراتة
serag.mustafa@cit.edu.ly

استلمت الورقة بتاريخ 2024/03/04
وقبلت بتاريخ 2024/3/20
ونشرت بتاريخ 2024/04/16

الكلمات المفتاحية: أمن المعلومات، الأمن السيبراني، التهديدات السيبرانية، الوعي بأمن المعلومات، القطاع المصرفي الليبي.

الملخص

أصبحت المعلومات وبنيتها التحتية من شبكات ومراكز بيانات ومنصات رقمية أمرا حيويا ومن أصول المؤسسات المالية التي يجب حمايتها والحفاظ عليها. وبالتالي فالموظف يجب أن يكون واعي بالتهديدات التي يمكن أن تتعرض لها المؤسسة وكيف يمكن أن يتعامل معها. فالموظف يعتبر الحلقة الأضعف في منظومة الحماية والأخطر ولذا وجب توعيته وتدريبه. تهدف هذه الدراسة إلى تحديد العوامل التي تؤثر على الوعي بأمن المعلومات، وتطوير خطط وسياسات أمن المعلومات لدى المصارف. مجتمع الدراسة عبارة عن عينة من موظفي المصارف الخاصة بمدينة مصراتة الليبية، في هذه الدراسة تم استخدام نموذج المعرفة والموقف والسلوك **(KBA) Knowledge, Attitude, Behavior** لدراسة الوعي بأمن المعلومات، وتم استخدام المنهج الكمي من خلال توظيف أداة الاستبيان حيث تم توزيع 111 استبيان على جميع موظفي المصارف المستهدفة، اشتمل الاستبيان على تسعة أقسام: القسم الأول تضمن المعلومات الديموغرافية، أما الأقسام الثمانية الباقية فتقيس مدى وعي الموظفين بأمن المعلومات من خلال تطبيق نموذج المعرفة والموقف والسلوك. وأظهرت نتائج الدراسة أن الاستبانة كانت موثوقة وثابتة حيث كان متوسط معامل الفاكرونباخ الموثوقية 70% تقريبا ويعتبر وفق المقبول والمعتمد مرجعيا، وتوصلت الدراسة إلى نتائج أهمها وجود علاقة ذات دلالة إحصائية بين وعي الموظفين بالمصارف الليبية بأهمية أمن المعلومات محل الدراسة، كما تم التأكد من أن الفرضيات العشرة المعتمدة في هذه الدراسة كانت ذات دلالة إحصائية باستثناء إدارة كلمات المرور التي أظهرت النتائج عدم وعي الموظفين بأهمية ادارتها، وتم قياس ذلك من خلال اختباري الانحدار البسيط ومعامل الارتباط بيرسون. وقدمت الدراسة مجموعة من التوصيات من أبرزها التأكيد على ضرورة وضع استراتيجية وطنية للأمن المعلومات للمصارف شاملة ومتكاملة، تركز على التحسين المستمر للوعي بأمن المعلومات للموظفين والعملاء، وتطوير القدرات الفنية والتنظيمية لهم.

1. المقدمة

تعتبر قضية أمن وحماية المعلومات من أهم القضايا في عصر الثورة الصناعية الرابعة. فقد أصبح نجاح المؤسسات والشركات يعتمد بشكل كبير على حماية المعلومات التي تمتلكها. وبالأخص المؤسسات المصرفية، فهي ليست بمعزل عن التحول الرقمي الذي يشهده العالم في شتى المجالات [1]. ومع ذلك، فإن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات معرضة للخطر من وقت لآخر فهي تواجه أنواعًا شتى من خروقات المعلومات وهجمات القرصنة. وتتعرض أيضًا لأنشطة إجرامية تستهدف تعطيل خدماتها وتدمير ممتلكاتها. ومع التطور المستمر أصبح الوعي بأمن المعلومات Information Security Awareness (ISA) مفهوما رئيسياً في حماية المعلومات، وعلى العكس من ذلك فإن المهاجمين يهتمون أكثر بتعزيز قدراتهم من خلال تطوير أساليب هجوم جديدة مختلفة؛ لذلك أصبح الأمن المعلوماتي مشكلة كبيرة يقلق منها كبار مسؤولي أمن المعلومات في كل مؤسسة [2]. من هذا المنطلق جاءت هذه الدراسة لتسلط الضوء على أهمية الوعي بالأمن المعلوماتي وخاصة في قطاع حيوي كقطاع المصارف ومعرفة مدى تطبيق المصارف للمعايير الدولية في أمن المعلومات ووضعها للسياسيات اللازمة لذلك وما يرافق ذلك من تدريب وتأهيل لموظفيها ليكونوا واعين بالتهديدات بل وقادرين على التعامل معها بجديه ووفق برنامج معتمد. وقد تم التركيز في هذه الدراسة على استخدام نموذج المعرفة والموقف والسلوك (KBA) لدراسة الوعي بأمن المعلومات، وتم استخدام المنهج الكمي من خلال توظيف أداة الاستبيان واشتملت الاستبانة على تسعة أقسام: القسم الأول تضمن المعلومات الديموغرافية، أما الأقسام الثمانية الباقية فتقيس مدى وعي الموظفين بأمن المعلومات من خلال تطبيق نموذج المعرفة والموقف والسلوك. وقد تضمنت الدراسة المحاور الرئيسة التالية المحور الأول مقدمة عن موضوع الدراسة، بينما المحور الثاني تطرق للإطار المنهجي للدراسة حيث تناول بالتفصيل إشكالية وتساؤلات واهداف الدراسة واهمية الدراسة وختم المحور بتفصيل المنهجية المتبعة في جمع وتحليل البيانات موضوع الدراسة، وتضمن المحور الثالث الإطار النظري للدراسة، بينما تم تحليل البيانات ومناقشة النتائج في المحور الرابع الجانب العملي، وأخيرا تم في المحور الخامس استعراض التوصيات والمقترحات المستقبلية لتحسين البحث في مجال الامن المعلوماتي.

أولاً/ الإطار المنهجي:

1. إشكالية الدراسة

يعد أمن المعلومات مكونا أساسيا من مكونات ومتطلبات أي تحول رقمي، حيث أن حماية البيانات والمعلومات والبنى التحتية ستكون مصدر قلق كبير للحكومة والعديد من القطاعات بما فيها القطاع المصرفي والقطاعات العامة. يواجه أمن المعلومات في مصارف العالم تحديات متزايدة خاصة وأن المصارف في ليبيا تفتقر إلى الموارد والخبرة اللازمة لتوفير تدابير أمن المعلومات المتقدمة مثل البرمجيات وموظفين أمن المعلومات، أشارت العديد من الدراسات إلى أن الحلقة الأضعف في دورة أمن المعلومات هي الموظفين أو العامل البشري [3]. وبالتالي من الضروري قياس مدى وعي ونضوج قدرات الامن السيبراني كجزء من الامن المعلوماتي والذي يهتم بمجموعة من الركائز لعل من أهمها: الركيزة الأولى: استراتيجية وسياسة الامن السيبراني، الركيزة الثانية: ثقافة الامن السيبراني والمجتمع، الركيزة الثالثة: بناء القدرات في مجال الامن السيبراني، الركيزة الرابعة: الأطر القانونية والتنظيمية، والركيزة الخامسة: المعايير والتقنيات [4].

هذه الدراسة تتناول قياس نضوج الموظفين وفهمهم لهذه الركائز وبناء على ماورد من توصيات في التقرير لمركز اكسفورد [4] تم تطوير وتحكيم الاستبانة الواردة في رسالة الماجستير [3] لتحقق اهداف هذه الدراسة.

2. تساؤلات الدراسة

تم إجراء الدراسة لإيجاد أجوبة على الأسئلة التالية:

- ما هي العوامل التي تؤثر على الوعي بأمن المعلومات؟
- ما هو الوضع الحالي للوعي بأمن المعلومات بين موظفين المصارف الخاصة في مصراتة؟
- كيف يمكن تطوير نموذج توعية بأمن المعلومات بين موظفين المصارف الخاصة في مصراتة؟

3. أهداف الدراسة

تهدف الدراسة إلى الوصول الى الأهداف التالية:

- التعرف على العوامل التي تؤثر على الوعي بأمن المعلومات على موظفين في المصارف الخاصة مصراتة
- دراسة الوضع الحالي للوعي بأمن المعلومات عند موظفي المصارف الخاصة في مصراتة
- تطوير نموذج توعية بأمن المعلومات بين موظفي المصارف الخاصة في مصراتة باستخدام نموذج (المعرفة، الموقف، السلوك)

4. أهمية الدراسة

بناء على ما قمنا به من استقصاء تعد هذا الدراسة من البحوث القليلة جدا التي تناقش درجة الوعي بأمن المعلومات لدى موظفي المصارف الليبية. هناك دراسات ناقشت درجة الوعي بأمن المعلومات ولكنها لم تقس نفس الفرضيات ونفس المجتمع .تم تصنيف هذا المحور الفرعي أهمية الدراسة الى الاهمية النظرية والاهمية العملية [3]:

أ. الأهمية النظرية

بناء على ما جاء في إشكالية الدراسة واهميته وما ورد في الدراسات ذات العلاقة والتي سنتطرق لها بالتفصيل في قسم الدراسات السابقة لاحقاً، يتضح جليا أهمية دراسة الوعي بأمن المعلومات وخطورته على الموظفين وتظهر الحاجة إلى وضع نموذج وإطار مفاهيمي يبين العلاقة بين الوعي بالأمن المعلوماتي لدى العينة المستهدفة ومدى تأثرها بعدد من العوامل البشرية التي تعتمد على معرفة وسلوك الموظف وما يترتب عليه من مواقف وقرارات حيال أي تهديد لأمن المعلومات. هذا النموذج المقترح يمكّن الباحثين من فهم العوامل البشرية التي تؤثر الوعي بالأمن المعلوماتي عموما والسيبراني خصوصاً.
تم تصميم هذا النموذج والاستبيان مع جوانب قريبة من ممارسات الموظفين من حيث المجالات مثل: إدارة كلمات المرور، استخدام البريد الإلكتروني، استخدام الإنترنت، استخدام وسائل التواصل الاجتماعي، الأجهزة المحمولة، معالجة المعلومات، والإبلاغ عن الحوادث التي تبين أن لها تأثيرًا كبيرًا على مدى معرفة الموظف وموقفه وسلوكه.

ب. الأهمية العملية

تكمن الأهمية العملية في هذه الدراسة في كونها تعتمد وتقيس الممارسات التي تؤثر على الوعي بأمن المعلومات لدى موظفي المصارف في مدينة مصراتة بدولة ليبيا، وخاصة مع ازدياد التعامل مع خدمات الدفع الالكتروني ومنصات وبوابات الخدمات الالكترونية وتحويل الأموال وظهور جيل جديد من الخدمات المالية الالكترونية والتي تسمى Fintech. كذلك أصبح من الضروري للمصارف العاملة الحصول على شهادات الاعتماد الخاصة بأمن المعلومات مثل ISO27001 وذلك للاعتراف الدولي والحصول على الخدمات المالية الدولية مثل التعامل مع الحولات المصرفية دولياً والذي يتطلب تطبيق معايير أمان دولية مثل شركة فيزا أو ماستر كارد وغيرها. ومن هنا فنقص الوعي لدى الموظفين ونقص التدريب سيزيد من المخاطر على المؤسسات بينما بناء القدرات والتدريب ووضع سياسات سيقلل من المخاطر، هذه الدراسة ستقيس مدى وعي الموظفين بأمن المعلومات كحالة دراسية تطبيقية بليبيا.

5. منهجية الدراسة

في هذه الدراسة تم اتباع أسلوب المنهج الكمي هو عبارة عن مجموعة من الخطوات التي تستخدم في إجراء عملية القياس، وذلك للقيام باختبار الفرضيات. من خلال توظيف أداة الاستبيان، اشتمل الاستبيان على تسعة أقسام: القسم الأول تضمن المعلومات الديموغرافية، أما الأقسام الثمانية الباقية فتقيس مدى وعي الموظفين بأمن المعلومات.

6. مجتمع وعينة الدراسة

يشمل مجتمع هذه الدراسة جميع موظفي ثلاثة مصارف خاصة في مصراتة، والبالغ عددهم (111) موظف. حيث تم استخدام أسلوب المسح الشامل لضمان دقة النتائج ولصغر حجم مجتمع الدراسة.

7. حدود الدراسة

- الحدود المكانية: تقتصر هذه الدراسة على المصارف التجارية الخاصة في مدينة مصراتة. دولة ليبيا.
- الحدود البشرية: تقتصر هذه الدراسة على الموظفين بالمصارف.
- الحدود الزمانية: تم إجراء هذه الدراسة في سنتي 2023-2024م.

8. الدراسات السابقة

أظهرت العديد من الدراسات السابقة أن برامج التوعية بأمن المعلومات تلعب دورًا هامًا في تعزيز الأمن المعلوماتي للمؤسسات العامة والخاصة، ومع ذلك الدراسات السابقة في مجال الوعي بأمن المعلومات والامن السيبراني تظل محدودة وفقا للبحث في قواعد ومحركات البحث المختلفة ومنها على سبيل المثال الدراسة التي نفذها Osman *سنة 2020 ركزت على قياس الوعي بالأمن السيبراني في الشركات الصغرى والمتوسطة، واظهرت النتائج* أنه هناك علاقة قوية وإيجابية بين قلة وعي الموظف بأمن المعلومات وزيادات التهديدات على المؤسسة، حيث تزيد مخاطر التهديدات السيبرانية مع عدم إدارة كلمات المرور بشكل صحيح، وعدم الاستخدام الصحيح للبريد الإلكتروني والإنترنت واستخدام سائل التواصل الاجتماعي والأجهزة المحمولة ومعالجة المعلومات داخل المؤسسات، وعدم الإبلاغ عن الحوادث. وبالتالي ركزت الدراسة على هذه المجالات لقياس مستوى الوعي بأمن المعلومات واقتراح بعض التوصيات لحل هذه المشكلة [3].

وفي نفس السنة 2020، أعد *Dharmawansa* وآخرون [2] دراسة تم خلالها تقييم الوعي العاملين في مجال أمن المعلومات في القطاع المصرفي في سريلانكا. اعتمدت هذه الدراسة على المنهج الكمي (استبيان) بنموذج (HAIS-Q). نتائج الدراسة أظهرت أن جميع المتغيرات المستقلة أثرت إيجابيا على المتغير المستقل التوعية بأمن المعلومات في القطاع المصرفي السيرلانكي.

كذلك في سنة 2020، عرض Stefaniuk في دراسته تقييم مدى فاعلية التدريب في تنمية وعي الموظفين في مجال الامن السيبراني، حيث تمت مقارنة مستوى الوعي لموظفي مؤسسة كبيرة في بولندا بين المشاركين في التدريب على أمن المعلومات وغير المشاركين. أظهرت النتائج فعالية التدريب في نشر المعرفة بأمن المعلومات وتأثيره الكبير على سلوك الموظفين في منطقة الدراسة. تشير هذه الدراسة إلى أهمية التدريب في توسيع المعرفة وتأثيره على السلوك في مجال أمن المعلومات [5].

في سنة 2022 قدمت زقوت وآخرين دراسة لتقييم وعي أعضاء هيئة التدريس بأمن المعلومات بجامعة الزاوية الدراسة استخدمت استبيانًا يتضمن 3 أقسام لتقييم وعي أعضاء هيئة التدريس بالأمن السيبراني [1]. وتوصلت الدراسة إلى نتائج أهمها وجود علاقة ذات دلالة إحصائية بين وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي في محل الدراسة. في المقابل لم تتضمن الدراسة بعض المتغيرات التي نرى من الضروري قياسها خاصة في قطاع المصارف.

مؤخرا في سنة 2023 قدمت Benqdara [6] برنامجًا تدريبيًا للتوعية بأمن المعلومات يهدف إلى تحسين معرفة الموظفين بهذا المجال وتعزيز سلوكياتهم في المؤسسات المالية الخاصة بليبيا. وخلصت النتائج إلى أهمية وفعالية تنفيذ البرامج التدريبية للتوعية بأمن المعلومات كوسيلة ليس فقط لتحسين المعرفة بأمن المعلومات ولكن أيضًا بشكل رئيسي له تأثير كبير على السلوك الفعلي للموظفين.

كذلك في سنة 2023 درس *Limna* وآخرون [7] العلاقة بين المعرفة بالأمن السيبراني والوعي وحماية الاختيار السلوكي بين مستخدمي الخدمات المصرفية عبر الهاتف المحمول في تايلاند. أظهرت النتائج أن المعرفة بالأمن السيبراني تؤثر بشكل كبير على الوعي بالأمن السيبراني وحماية الاختيار السلوكي.

مؤخرا في سنة 2023 قام المركز العالمي لبناء القدرات السيبرانية التابع لجامعة أكسفورد بإعداد تقرير يستعرض القدرات الليبية في مجال الامن السيبراني، حيث تم اجراء عديد المقابلات الشخصية مع عدد من المتخصصين في مجال الامن السيبراني في عدد من المؤسسات العامة في الدولة الليبية وبعض مؤسسات القطاع الخاص وصف التقرير الوضع الحالي، تم اقترح عدد من التوصيات منها ما يخص القطاع المالي والمصرفي لتغطية الفجوة بهذا القطاع [4]:

- السعي إلى تعزيز مستوى الوعي بأمن المعلومات وأولوية الأمن السيبراني واستخدام ممارسات آمنة في هذا المجال ضمن الأجهزة الحكومية والقطاع الخاص من خلال التوعية والتدريب.
- تطوير الاستبيانات لتقييم مستوى المعرفة بمسألة الامن السيبراني بشكل أكثر انتظاما في البلاد وتحليل نتائجها بمرور الوقت لتحديد مدى فعالية جهود التوعية ضمن مختلف شرائح المجتمع.

وبناء على ماورد من توصيات في التقرير [4]، تم تطوير الاستبانة الواردة في رسالة الماجستير [3].

9. الفرضيات والإطار المفاهيمي لدراسة

تم تطوير فرضيات الدراسة الثلاثة الأولى المعرفة، الموقف، السلوك بناءً على الدراسة التي أُجريت بواسطة Osman[3]، وكما هو مبين بالإطار المفاهيمي للدراسة بالشكل (1)، وعلى النحو التالي:

الفرضية الأولى: معرفة الموظفين بالسياسات والإجراءات والبروتوكولات لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

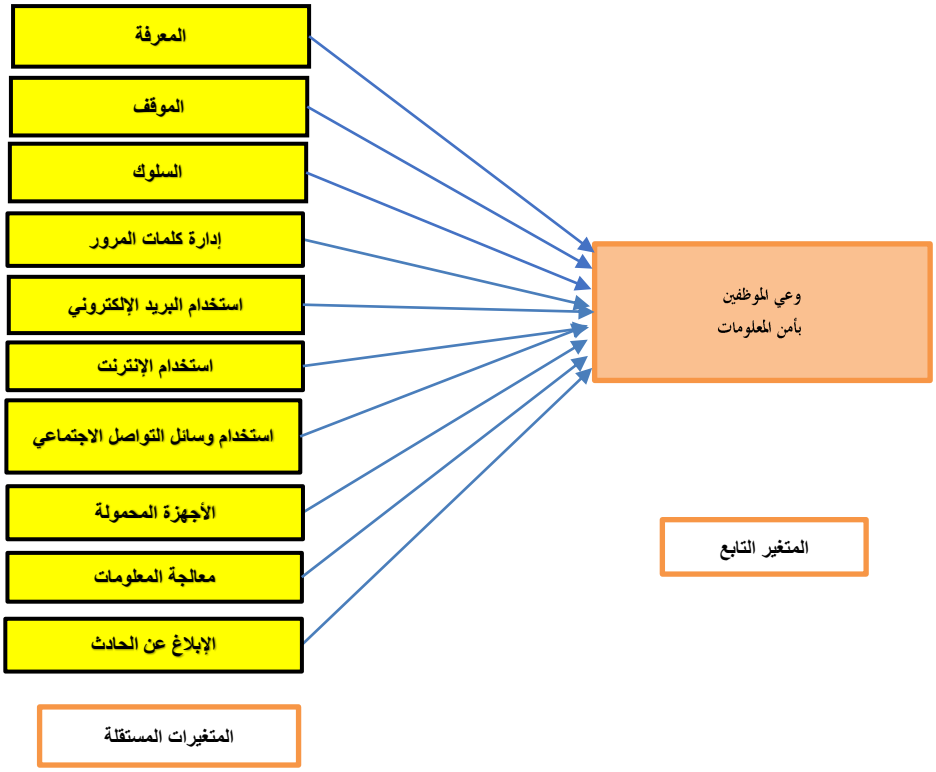
الفرضية الثانية: موقف الموظفين تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

الفرضية الثالثة: سلوك الموظفين تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

الفرضية الرابعة: ممارسة الموظفين في إدارة كلمات المرور لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف في مصراتة.

الفرضية الخامسة: ممارسة الموظفين في استخدام البريد الإلكتروني كمجال تركيز له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

الفرضية السادسة: ممارسة الموظفين في استخدام الإنترنت لها تأثير سلبي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.
الفرضية السابعة: ممارسة الموظفين في استخدام وسائل التواصل الاجتماعي لها تأثير سلبي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.
الفرضية الثامنة: ممارسة الموظفين في استخدام الهاتف المحمول لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.
الفرضية التاسعة: ممارسة الموظفين في التعامل مع المعلومات لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.
الفرضية العاشرة: ممارسة الموظفين في الإبلاغ عن الحوادث لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.



الشكل (1) الإطار المفاهيمي

10. مراحل الدراسة

تتكون خارطة طريق منهجية الدراسة من خمس مراحل كما هو موضح في الشكل (2)، المرحلة الأولى تحديد المشكلة وضع الأهداف والتساؤلات والفرضيات، تتضمن المرحلة الثانية الدراسات السابقة، أمن المعلومات، الأمن السيبراني، نموذج المعرفة والموقف والسلوك بينما في المرحلة الثالثة، تتم تحديد نوع المنهجية، وطريقة جمع البيانات، وتحديد المجتمع، تحديد حجم العينة، اختيار أداة القياس وفي المرحلة الرابعة تتم مناقشة النتائج، وفي المرحلة الأخيرة الاستنتاجات والتوصيات.

الشكل (2) خارطة الطريق لمنهجية الدراسة.

ثانياً /الإطار النظري:

1. أمن المعلومات

هو السياسات والإجراءات التي يتم اتخاذها لحماية المعلومات والبيانات من الوصول غير المصرح به والتلاعب بها او تدميرها، ويشمل هذا المجال العديد من الأمور مثل الحماية من المخاطر الطبيعية مثل الزلازل والفيضانات والحرائق أو المخاطر العامة مثل انقطاع الانترنت أو الكهرباء، ويشمل المخاطر السيبرانية مثل هجمات التنصت والاحتيال الالكتروني وقطع الخدمة أو الهجمات الخبيثة على أنظمة المعلومات والشبكات باستخدام الفيروسات والديدان [2].

2. الأمن السيبراني

الأمن السيبراني هو حالة خاصة من أمن المعلومات، ويختص بحماية الأنظمة والشبكات والبرامج والأجهزة المتصلة بالإنترنت من المخاطر والتهديدات الإلكترونية او السيبرانية. تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها [8]. الجدول (1) أدناه يوضح الفروقات بين أمن المعلومات والأمن السيبراني.

الجدول (1) مقارنة بين أمن المعلومات والأمن السيبراني **[8]**

الخاصية	أمن المعلومات	الأمن السيبراني
النطاق	يركز على حماية المعلومات بشكل عام، بغض النظر عن شكلها أو مكان تخزينها وتشمل المعلومات الورقية.	يركز على حماية المعلومات الرقمية فقط، مثل البيانات المخزنة على أجهزة الكمبيوتر أو الأجهزة المحمولة أو الشبكات.
التهديدات	تشمل التهديدات التقليدية مثل السرقة والتلف والضياع، بالإضافة إلى التهديدات الإلكترونية مثل البرامج الضارة والهجمات الإلكترونية.	تركز على التهديدات الإلكترونية، مثل البرامج الضارة والهجمات الإلكترونية، بما في ذلك هجمات التصيد الاحتيالي، والهندسة الاجتماعية، والهجمات على البنية التحتية.
الحلول	تشمل حلول أمن المعلومات الإجراءات الإدارية والفنية، مثل: سياسات أمن المعلومات، التدريب على الوعي بالأمان، التشفير، النُسخ الاحتياطي للبيانات.	تشمل حلول الأمن السيبراني الإجراءات الإدارية والفنية، مثل: جدران الحماية، أنظمة الكشف عن التسلل، أنظمة منع التطفل، التحديثات الأمنية.

3. التهديدات الإلكترونية والهجمات السيبرانية وطرق الوقاية منها

التهديدات السيبرانية هي أساليب وتقنيات وبرمجيات تهدف الى الاضرار بعناصر أمن المعلومات (السرية وسلامة المعلومات وتوافر الخدمة والمصادقة وعدم الانكار)، والجدول (2) أدناه يوضح طرق الوقاية من التهديدات الإلكترونية والهجمات السيبرانية للحفاظ على أمن المعلومات من خلال الحفاظ على سرية وسلامة المعلومات وتوافرها وعد انقطاعها وكذلك معرفة هوية صاحب المعلومات وضمان عدم الانكار لمن تعامل مع هذه المعلومات.

الجدول (2) التهديدات الإلكترونية والهجمات السيبرانية وطرق الوقاية منها [1][3].

التهديد	الوصف	طرق الوقاية
برامج الضارة	برامج مصممة لإلحاق الضرر بالنظام أو البيانات.	استخدام برامج مكافحة الفيروسات وجدران الحماية. تحديث البرامج بشكل منتظم.
الهندسة الاجتماعية	تقنيات لخداع المستخدمين للكشف عن معلومات حساسة أو اتخاذ إجراءات غير آمنة.	نشر الوعي بمخاطر الهندسة الاجتماعية، تدريب الموظفين على كيفية التعرف على محاولات الاحتيال، وعدم النقر على الروابط المشبوهة أو عدم تنزيل التطبيقات الا من مواقع موثوقة واستخدام تقنيات المصادقة الثنائية.
هجمات التصيد الاحتيالي	تهدف هذه الهجمات إلى خداع المستخدمين واستدراجهم للكشف عن معلومات شخصية حساسة أو مالية، مثل كلمات المرور، وأرقام الحسابات المصرفية، ومعلومات البطاقات الائتمانية. وتكون الهجمات عبر رسائل بريد إلكتروني أو رسائل نصية أو مواقع ويب مصممة لخداع المستخدمين للكشف عن معلومات حساسة.	توخي الحذر عند فتح رسائل البريد الإلكتروني أو النقر على الروابط، التحقق من صحة عنوان URL قبل إدخال أي معلومات. استخدام كلمات مرور قوية وفريدة من نوعها وعدم تبادل كلمات المرور أو مشاركتها مع الغير.
هجمات(DDoS)	هجمات تهدف إلى إغراق خادم أو شبكة بالطلبات، مما يجعلها غير متوفرة للمستخدمين الشرعيين.	استخدام أنظمة الكشف عن التسلل ومنع التطفل. استخدام تقنيات التوازن بين الأحمال. تحديث البرامج بشكل منتظم.

4. نموذج المعرفة-الموقف-السلوك

تم في هذه الدراسة استخدام نموذج المعرفة والموقف والسلوك (KBA)لدراسة الوعي بأمن المعلومات، وفقًا لـ أورده **Osman**[3]، فقد عرف المعرفة والموقف والسلوك كالتالي:

أ. المعرفة

تشير إلى المعلومات والمفاهيم التي يمتلكها الفرد، حيث تلعب دورًا مهمًا في تحديد موقف وسلوك المستخدم. وبالتالي فمعرفته بطبيعة التهديدات والمخاطر تجنبه الوقوع بها.

ب. الموقف

يشير إلى الاتجاه العاطفي للشخص تجاه الموضوع، فإذا كان الموقف إيجابيًا فمن المحتمل أن يقوم الشخص باتخاذ إجراءات صحيحة وإذا كان الموقف سلبيًا فمن المحتمل أن يقوم باتخاذ قرارات غير صحيحة، وبالتالي يمكن أن يقع ضحية التصيد أو الاحتيال أو هجمات الهندسة العكسية.

ج. السلوك

يشير إلى التصرفات والإجراءات التي يتبعها الفرد فيما يتعلق بأمن المعلومات. يمكن أن يشمل ذلك استخدام كلمات مرور قوية وتغييرها بانتظام، وعدم مشاركتها وتحديث البرامج والأنظمة بأحدث التحديثات الأمنية، وتجنب مشاركة المعلومات الشخصية عبر وسائل غير آمنة.

ثالثاً/الجانب العملي للدراسة:

1. الجانب الميداني للدراسة

يتناول هذا الجانب تجميع البيانات من خلال الزيارات الميدانية للمصارف المستهدفة في هذا الدراسة.

2. آلية جمع وتحليل البيانات

بعد الاطلاع على الدراسات السابقة التي تتعلق بموضوع الدراسة، قام الباحثان بتصميم أداة الدراسة ومن تم تحكيمها من خلال عرض الاستبيان على عدد من الخبراء في المجال، حيث شمل الاستبيان على تسعة اقسام: القسم الأول تضمن المعلومات الديموغرافية، أما الأقسام الثمانية الباقية فتقيس مدى وعي الموظفين بأمن المعلومات من خلال تطبيق نموذج المعرفة والموقف والسلوك.

تم توزيع الاستبيان على جميع موظفي المصارف المستهدفة، كما تم تحليل البيانات باستخدام أداة SPSS للتحليل الإحصائي وإيجاد العلاقة بين المتغير التابع والمتغيرات المستقلة ومن ثم تحقق من صحة الفرضيات من عدمها باستخدام المقاييس الإحصائية التي يتم توظيفها عن طريق أداة SPSS.

3. تنظيف البيانات

تعتبر عملية تنظيف البيانات Data Cleaning مهمة لضمان جودة البيانات وسهولة التحليل دون فقدان أي متغيرات يمكن أن تقلل من جودة البيانات التي تم جمعها. تم إجراء عملية تنظيف البيانات لاكتشاف التناقضات في البيانات وتصحيح الأخطاء، وتم توزيع عدد من الاستبيانات على مختلف الموظفين في المصارف الخاصة في مدينة مصراتة على مدى أسبوع ونصف لضمان الوصول إلى أكبر عدد في وقت قصير فقد تم جمع إجمالي عدد 87 استبيان. وتم فحص الاستبيان يدويا للتأكد من عدم وجود بيانات مفقودة، وفي الحالات التي لم يكمل فيها الاستبيان مستكملا يتم حذف الاستبيان، بعد فحص الاستبيانات يتطلب معالجة إضافية للبيانات وترميزها قبل تحليل البيانات.

4. معالجة البيانات والترميز

تتطلب طبيعة الاستبيان معالجة إضافية للبيانات حيث يتم ترميز البيانات ليسهل التعامل معها بواسطة أداة التحليل الاحصائي، عندما يتم وضع الاوزان في مقياس ليكرت الخماسي في المدى من موافق بشدة (5) الى غير موافق بشدة (1)، بينما محايد تأخذ (3) وموافق (4) وغير موافق (2). يجب قراءة سؤال (عنصر) الاستبيان جيدا لوضع الوزن المناسب عند الترميز. كما أن بعض عناصر الاستبيان تحتاج إلى ترميز عكسي وذلك عندما تكون صياغة عنصر الاستبيان بشكل سلبي، تعتبر عملية الترميز العكسي مهمة لضمان موثوقية بيانات الاستبيان، تتم عملية الترميز العكسي تلقائيًا في برنامج **SPSS** للعناصر المشار إليها للترميز العكسي، في هذه الخطوة يتم تحويل القيم كما هو موضح بالجدول (3) على النحو التالي:

الجدول (3) قيم الترميز العكسية

القيمة السابقة	القيمة الجديدة
1	5
2	4
3	نفس القيمة
4	2
5	1

بالإضافة إلى ذلك، يعد ترميز المتغيرات خطوة مهمة لأنه يتيح سهولة ومعالجة البيانات في برنامج SPSS، يفرض البرنامج بعض الشروط على أسماء المتغيرات مثل عدم وجود مسافات وأن يكون الحرف الأول حرفًا أو أحد الأحرف @ أو # أو $، ويمكن أن تكون مزيج من مجموعة من الحروف والأرقام والأحرف التي لا تحتوي على علامات ترقيم ونقطة (.) على الرغم من إمكانية إدخال اسم المتغير باللغة العربية، إلا أن خطوة التشفير العكسية في الجزء السابق تتم لتسهيل إدخال البيانات وعرضها في الدراسة.

5. اختبار الموثوقية

تم إجراء اختبار الموثوقية (Reliability Testing) اعتمادا على معامل ألفا كرونباخ (Cronbach alpha) لكل العناصر لتقييم الاتساق الداخلي للأداة، حيث يتم استخدام ألفا كرونباخ لتقدير درجة التباين لدرجات الاختبار وتتراوح عادةً بين 0 و1. وفقًا لـ (*Osman, A*) [3]، تشير قيم ألفا كرونباخ إلى موثوقية عنصر الاستبيان في قياس المتغير المقصود، تشير القيم إلى موثوقية أداة الدراسة يمكن أن تكون القيم كما يلي: 0.90 وما فوق تشير إلى موثوقية ممتازة، و0.70-0.90 تشير إلى موثوقية عالية؛ 0.50-0.70 تشير إلى موثوقية معتدلة، وتشير 0.50 وما دونها إلى موثوقية منخفضة.
تشير النتيجة الموضحة في الجدول (4) أدناه والتي تتراوح بين 0.60 إلى 0.90 إلى موثوقية عالية ومعتدلة، ولم يتم حذف أي عناصر من التحليل ومن هنا نستنتج أن الاستبانة ذات صدق وثبات عالي.

الجدول (4) قيمة ألفا كرونباخ لجميع العناصر

العنصر	الموثوقية	ألفا كرونباخ	عدد الاسئلة
كلمات المرور	عالية	0.709	9
استخدام البريد الإلكتروني	معتدلة	0.583	9
استخدام الإنترنت	معتدلة	0.691	9
استخدام وسائل التواصل الاجتماعي	معتدلة	0.564	9
الأجهزة المحمولة	معتدلة	0.684	9
معالجة المعلومات	معتدلة	0.677	9
الإبلاغ عن الحادث	عالية	0.758	9
المعرفة	معتدلة	0.657	21
الموقف	عالية	0.731	21
السلوك	عالية	0.788	21

6. نتائج تحليل البيانات الديموغرافية

تتمثل الخطوة الأولى في تحليل البيانات في فحص المعلومات الديموغرافية للمستجيبين، وهذا يمكننا من الحصول على نظرة عامة كاملة على المستجيبين للاستبيان، تتضمن معلومات المستجيب كالتالي: العمر والجنس ومستوى التعليم والقسم ومستوى الإدارة وسنوات العمل في المصرف وعدد الموظفين في المصرف. يتم تقييم المعلومات الديموغرافية من حيث التكرار والنسبة المئوية في البيانات، يقدم القسم التالي نتائج التوزيع التكراري والنسبة المئوية للمشاركين في المسح.
كما هو مبين في الجدول (5) أدناه، كان المشاركون الذكور هم الغالبية في الدراسة حيث شكلوا 82.8٪ (72 من 87 مستجيبًا) من إجمالي العينة، يليهم 17.2٪ (17 من أصل 87 مستجيبًا) من الإناث، بالإضافة إلى ذلك فإن غالبية المشاركين في الفئة العمرية بين 20 و30 عامًا وتتكون من 72.4٪ (63 مشاركًا من 87) من إجمالي العينات التي تم جمعها والتي تمثل أعلى نسبة للمستجيبين في هذه الدراسة. تليها المجموعة الثانية من المستجيبين، الذين يشكلون 24.1٪ من إجمالي المستجيبين الذين تتراوح أعمارهم بين 31 و40 عامًا (21 مشاركًا من 87) من إجمالي العينات التي تم جمعها، علاوة على ذلك فإن المستجيبين الذين تتراوح أعمارهم بين 41 إلى 50 عامًا شكلوا 2.3٪ من إجمالي المستجيبين (2 مشاركًا من 87) أخيرًا، كان المشاركون الذين تزيد أعمارهم عن 50 عامًا في هذه الدراسة 1.1٪ فقط (1 فقط من أصل 87 مشاركًا). وكما هو موضح بالجدول (5) فيما يتعلق بأعلى المؤهلات الأكاديمية فإن 71.3٪ من المستجيبين (62 مستجيبًا من 87) خريجو جامعة بدرجة البكالوريوس، و9.2٪ من المستجيبين (8 مستجيبًا من 87) حاصلون على شهادات عليا، و19.5٪ من المستجيبين (17مشاركًا من أصل 87) لديهم شهادات دبلوم. فيما يتعلق بعدد سنوات العمل في المصارف المستهدفة، أشار معظم المستجيبين 69.0٪ (60 مشاركًا من 87) إلى أنهم يعملون منذ 1-5 سنوات وأن 16.1٪ (14 مشاركًا من أصل 87) يعملون منذ أكثر من خمس سنوات. بينما 14.9٪ فقط (13 مشاركًا من أصل 87) يعملون منذ أقل من عام واحد.

الجدول (5) توزيع عينة الدراسة حسب الخصائص الشخصية والوظيفية.

الجنس	العدد	نسبة مئوية
ذكر	72	%82.8
أنثى	15	%17.2
الإجمالي	87	%100
عمر الموظفين	العدد	نسبة مئوية
20-30	63	%72.4
31-40	21	%24.1
41-50	2	%2.3
أكبر من 51	1	%1.1
الإجمالي	87	%100
المؤهلات الأكاديمية	العدد	نسبة مئوية
الدبلوم	17	%19.5

البكالوريوس	62	%71.3
الدراسات عليا	8	%9.2
الإجمالي	87	%100
سنوات العمل	العدد	نسبة مئوية
أقل من سنة	13	%14.9
من سنة إلى خمس	60	%69.0
أكثر من خمس	14	%16.1
الإجمالي	87	%100
الجنس	العدد	نسبة مئوية
ذكر	72	%82.8
أنثى	15	%17.2
الإجمالي	87	%100

نظرًا لأن هدف هذا الدراسة هو قياس الوعي بأمن المعلومات في عدد من المصارف الخاصة في مصراتة على وجه التحديد، كان من المهم معرفة عدد الموظفين العاملين في هذه المصارف، والجدول (6) يبين عدد ونسبة الموظفين لكل مصرف استهدف بالدراسة ضمن البيانات الديموغرافية التي جمعها هذا الدراسة

الجدول (6) عدد الموظفين بالمصارف.

عدد الموظفين	العدد	نسبة مئوية
المصرف أ	56	%50.45
المصرف ب	25	%22.52
المصرف ج	30	%27.03
الإجمالي	111	%100

7. نتائج تحليل البيانات الديموغرافية

تم إجراء تحليل الانحدار البسيط لقياس الدلالة الإحصائية ومعامل التحديد ومدى تأثير المتغيرات المستقلة على المتغير التابع في دراستنا.
الجدول (7) يعطي ملخصاً للعلاقة بين المتغيرات المستقلة والمتغير التابع يبين التأثير لكل متغير مستقل على المتغير التابع بواسطة تحليل الانحدار البسيط، يوضح هذا الملخص مدى قوة ودقة العلاقة بين المتغيرات وما إذا كانت تلك العلاقة ذات دلالة إحصائية أم لا. إحدى المؤشرات الهامة المستخدمة في ملخص النموذج هي قيمة الدلالة الإحصائية "sig F" و القيمة الاحتمالية (p-value) المرتبطتان بالاختبار الإحصائي للفرضية ويجب ان تكون قيمة p أقل من 0.05 لتشير إلى نتائج ذات دلالة إحصائية و R square هو معامل التحديد أو الترابط ويستخدم لتقييم مدى قوة النموذج في تفسير التباين في المتغير التابع من خلال المتغيرات المستقلة، يتراوح قيم R square من 0 إلى 1، حيث تشير القيم الأعلى إلى أن المتغير المستقل يؤثر ويرتبط بنسبة كبيرة مع المتغير التابع، على سبيل المثال إذا كان0.8 = R square ، فإن 80٪ من التغير في المتغير التابع يمكن تفسيره بواسطة المتغير المستقل [9].
النتائج في الجدول (7) تظهر قيم الدلالة الإحصائية و معامل التحديد للعلاقة بين المتغير التابع والمتغيرات المستقلة من خلال الفرضيات العشرة التي تم وضعها بهذه الدراسة. وسيأتي تفصيلها فيما يلي في بند الفرضيات.
ومن أجل فحص التأثير لكل من المتغيرات المستقلة في النموذج تم فحص جدول المعاملات، قيمة معامل الانحدار(**coefficients**) هي قيمة تحدد العلاقة بين المتغير المستقل والمتغير التابع، يتم حساب قيمة معامل الانحدار البسيط باستخدام تقنية الانحدار الخطي، ويتم استخدامها لتوقع قيم المتغير التابع بناءً على قيم المتغير المستقل، وتشير قيمة معاملات بيتا **Coefficients Beta** إلى مقدار التأثير الذي يمارسه المتغير المستقل على المتغير التابع وتتراوح قيم بيتا **(Beta)** بين -1 و1، فإن كانت قيمة **Beta** موجبة يشير ذلك إلى وجود علاقة إيجابية بين المتغيرين، أي أن زيادة قيمة المتغير المستقل تؤدي إلى زيادة قيمة المتغير التابع، وإذا كانت قيمة **Beta** سالبة، فإن ذلك يشير إلى وجود علاقة سلبية بين المتغيرين، أي أن زيادة قيمة المتغير المستقل تؤدي إلى انخفاض قيمة المتغير التابع، وكلما كانت قيمة **Coefficients Beta** أكبر، كلما كانت العلاقة بين المتغيرين أقوى .
كما تم اختبار العلاقة الخطية من خلال اختبار معامل ارتباط بيرسون.**(Pearson Correlation Coefficient)** تشير نتيجة التعدد الخطي إلى وجود تعدد خطي موجب بين المتغيرات، وهو أمر مهم للتأكد من أن المتغيرات التابعة التي تم اختبارها مرتبطة ببعضها البعض، وفقا لـ [3] لقياس قوة الارتباط الخطي بين متغيرين ويرمز له بالرمز **r** يتراوح معامل ارتباط بيرسون **r** من +1 إلى -1 ، إذا كانت قيمة **R** هي 0، فهذا يشير إلى عدم وجود ارتباط بين المتغيرين، تشير القيمة الموجبة إلى ارتباط موجب بينما تشير القيمة السالبة إلى ارتباط سلبي كما تشير إلى اتجاه العلاقة بين المتغيرات، كلما زادت قيمة **r** بغض النظر عن الإشارة تشير إلى ارتباط أقوى، في تحليل الانحدار يجب تقديم درجة معينة من الارتباط في المتغيرات، وفي دراستنا تتراوح قيم ارتباط بيرسون بين -0.268 إلى 0.756 مما يشير إلى وجود ارتباط متوسط بين المتغيرات، وتشير النتيجة إلى مستوى مقبول من العلاقة الخطية بين المتغيرات وفي الجدول (7) نبين قيم معامل الارتباط بيرسون ونتائج إجراء اختبار تحليل الانحدار البسيط.

الجدول (7) نتائج إجراء اختبار تحليل الانحدار البسيط ومعامل بيرسون

الفرضية	الدلالة الإحصائية	معامل الارتباط بيرسون	معامل التحديد	المعاملات الموحدة بيتا	النتيجة
المعرفة	.000	.713**	.508	.713	يدعم
الموقف	.000	.636**	.405	.636	يدعم

السلوك	.000	.751**	.564	.751	يدعم
إدارة كلمات المرور	.250	.125	.016	.125	غير مدعومة
استخدام البريد الإلكتروني	.012	-.268*	.072	-.268	يدعم
استخدام الإنترنت	.000	.472**	.223	.472	يدعم
استخدام وسائل التواصل الاجتماعي	.008	.283**	.080	.283	يدعم
استخدام الأجهزة المحمولة	.000	.655**	.430	.655	يدعم
معالجة المعلومات	.000	.413**	.171	.413	يدعم
الإبلاغ عن الحوادث	.000	.756**	.571	.756	يدعم

1. الفرضية الأولى

أظهرت نتائج الفرضية الأولى أن المتغير المستقل (المعرفة) له علاقة إيجابية بالوعي الأمني السيبراني وتشير النتيجة إلى أن زيادة المعرفة ستؤدي إلى زيادة الوعي بأمن المعلومات، القيمة **p = 0.00** وهي أقل من 0.05 تشير إلى النتيجة ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 50٪ من التغير في المتغير التابع، وهو الوعي بأمن المعلومات. ويعني ذلك أن المتغير التابع يمكن التأثير عليه بواسطة المتغير المستقل، وهو المعرفة. وبالتالي نخلص الى أن معرفة الموظفين بالسياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

2. الفرضية الثانية

الموقف وهو مؤشر آخر في النموذج، حيث أشارت النتيجة إلى وجود علاقة إيجابية بين موقف الموظف والوعي بأمن المعلومات وهذا يعني أن الزيادة في موقف الموظف بمقدار 0.636 ستؤدي إلى زيادة الوعي بأمن المعلومات وتشير القيمة **p =0.00** وتقل عن 0.05 المرجعية، وبالتالي تكون النتيجة ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 40٪ من التغير في المتغير التابع (الوعي بأمن المعلومات) حدث بسبب المتغير المستقل الموقف. مما يعني أن الموقف يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن الموقف الإيجابي للموظفين تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات لدى عينة الدراسة.

3. الفرضية الثالثة

السلوك هو المتغير الثالث الذي تم اختباره في النموذج، أشارت النتائج إلى أن السلوك له علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن السلوك يعد مؤشرا هاما حيث أن زيادة سلوك مع الوعي بأمن المعلومات يؤدي إلى زيادة مستوى أمن المعلومات بمقدار 0.751 تشير القيمة **p=0.00** وهي أقل من 0.05 إلى نتائج ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 56٪ من التغير في المتغير التابع، وهو الوعي الأمني السيبراني، يمكن تفسيره أو يمكن التأثير عليه بواسطة المتغير المستقل، وهو السلوك. مما يعني أن السلوك يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن الفرضية الثالثة التي تشير إلى أن سلوك الموظفين الايجابي تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

4. الفرضية الرابعة

أظهرت نتائج الفرضية الرابعة أن المتغير المستقل (إدارة كلمات المرور) ليس له علاقة (لا سلبيه ولا ايجابيه) مع المتغير التابع الوعي بالأمن المعلوماتي كما تشير قيمة الدلالة الإحصائية **p=0.250** وهي أعلى من 0.05 إلى أنه لا يوجد دلالة إحصائية بالتالي فإن فرضية إدارة كلمات المرور غير مدعومة. بالرغم من أن الدراسات السابقة إشارة الى وجود تأثير إيجابي بين الوعي بالأمن السيبراني وحسن إدارة كلمات المرور. ولكن في هذه الدراسة لم يكون التأثير واضح. قام البحاث بعمل مقابلات مع عينة من الموظفين بالمصارف المستهدفة 7 موظفين بكل مصرف ومناقشتهم حول كيفية ادارتهم لكلمات المرور وبيان مدى معرفتهم بإدارة الكلمات بشكل أمن وموقفهم من مشاركة كلمات المرور مع زملائهم أو اختيار كلمات سهلة التذكر. وكانت الإجابات لحوالي 70% منهم غير واضحة وليس لديهم معرفة بكيفية إدارة كلمات المرور وهذا يفسر اجاباتهم غير الدقيقة في الاستبيان.

5. الفرضية الخامسة

أظهرت نتائج الفرضية الخامسة أن المتغير المستقل (استخدام البريد الإلكتروني) له تأثير سلبي على الوعي بأمن المعلومات، أشارت النتيجة إلى وجود علاقة عكسية بين استخدام البريد الإلكتروني والوعي بأمن المعلومات، ويشير النموذج أيضًا إلى أن استخدام البريد الإلكتروني يعد مؤشرًا مهمًا حيث أن زيادة استخدام البريد الإلكتروني بين موظفي المصارف سيؤدي إلى انخفاض الوعي بأمن المعلومات بمقدار 0.268 وتشير القيمة **p=0.012** ، وهي أقل من 0.05، إلى نتائج ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 7% من التغير في المتغير التابع، وهو الوعي الأمني السيبراني، يمكن تفسيره أو يمكن التأثير عليه بواسطة المتغير المستقل، وهو استخدام البريد الإلكتروني. مما يعني أن استخدام البريد الإلكتروني يعد مؤشرًا مهمًا بالنسبة للتوعية بأمن المعلومات، ووفقًا للتحليل الإحصائي أظهرت الفرضية الخامسة وجود تأثير سلبي غير متوقع لممارسة الموظفين في استخدام البريد الإلكتروني على الوعي بأمن المعلومات. على الرغم من أن الفرضية كانت تفترض وجود تأثير إيجابي، مما يدل هذا على عدم توفر الوعي لدى الموظفين بكيفية استخدام البريد الالكتروني وادارته بشكل آمن. وهذا ناجم عن عدم التدريب الكافي على الإدارة السليمة للبريد الالكتروني وعدم الوقع ضحية التهديدات السيبرانية، كما لاحظ البحاث عند اجراء المقابلات وعدم وجود سياسات صارمة لاستخدام البريد الإلكتروني وهذا يعني وجود قلة وعي في استخدامهم للبريد الإلكتروني.

6. الفرضية السادسة

استخدام الانترنت هو المتغير السادس الذي تم اختباره في النموذج، أظهرت النتائج أن استخدام الانترنت بشكل مسؤول له علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن استخدام الانترنت يعد مؤشرا هاما حيث أن استخدام الانترنت بضوابط يؤدي إلى زيادة أمن المعلومات بمقدار 0.472، وتشير القيمة **p=0.00** مما يعني أن النتيجة ذات دلالة إحصائية، بينما معامل التحديد **(R Square)** يشير إلى أن 22٪ من التغير في المتغير التابع

يمكن التأثير عليه بواسطة المتغير المستقل بنسبة 22٪. وبالتالي فإن الفرضية السادسة والتي تشير إلى أن استخدام الموظفين للأنترنت بشكل مسؤول والالتزام بسياسات المؤسسة في مجال أمن المعلومات له تأثير إيجابي على الوعي بأمن المعلومات على عينة الدراسة. على الرغم من الفرضية الأساسية التي تفترض أن ممارسة الموظفين في استخدام الإنترنت لها تأثيرًا سلبيًا، إلا أن النتائج التحليلية للدراسة أظهرت وجود تأثير إيجابي ملحوظ على وعي الموظفين بأمن المعلومات في المصارف الخاصة في مصراتة. ويمكن تفسير التأثير الإيجابي الذي تم العثور عليه مرتبطًا بتطبيق إجراءات وسياسات أمنية في المصارف الخاصة في مصراتة، مما يساهم في تعزيز وعي الموظفين بأمن المعلومات.

7. الفرضية السابعة

استخدام وسائل التواصل الاجتماعي هو المتغير السابع الذي تم اختباره في النموذج. تم التركيز هنا على فهم الموظفين لأهمية حماية حساباتهم ومراجعة الاعدادات. كما تم التركيز على موقف الموظفين وسلوكهم اتجاه ما ينشر من خصوصية العمل للعامة أم لا. أشارت النتائج إلى أن حسن استخدام وسائل التواصل الاجتماعي له علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن استخدام وسائل التواصل الاجتماعي بشكل مسؤول يعد مؤشرا هاما حيث أن استخدام وسائل التواصل الاجتماعي بشكل مسؤول يؤدي إلى زيادة الوعي بأمن المعلومات بمقدار 0.28 ، وتشير القيمة **p=0.008** إلى نتائج ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 8% من التغير في المتغير التابع، يمكن التأثير عليه بواسطة المتغير المستقل، وهو استخدام وسائل التواصل الاجتماعي. مما يعني أن استخدام وسائل التواصل الاجتماعي بشكل مسؤول بعيدا عن الاضرار بموارد جهة العمل يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن الفرضية السابعة الذي يشير إلى أن استخدام وسائل التواصل الاجتماعي الموظفين وفق ضوابط وسياسات المؤسسة له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة. وعلى الرغم من أن الفرضية الأساسية تنص على أن استخدام الموظفين وسائل التواصل الاجتماعي لديه تأثيرًا سلبيًا، إلا أن النتائج التحليلية للدراسة أظهرت وجود تأثير إيجابي ملحوظ على وعي الموظفين بأمن المعلومات في المصارف الخاصة في مصراتة. ويمكن تفسير التأثير الإيجابي الذي تم الحصول عليه مرتبطًا بتوفر سياسات ولوائح تنظيمية وثقافة مجتمعية بشأن التأكيد على أهمية استخدام وسائل التواصل الاجتماعي بشكل مسؤول وتوخي الحذر من التهديدات السيبرانية المختلفة واستخدام كل السبل التقنية لحماية موارد المؤسسة، مما يسهم في تعزيز وعيهم بأمن المعلومات في المصارف الخاصة في مصراتة.

8. الفرضية الثامنة

الأجهزة المحمولة هو المتغير الثامن الذي تم اختباره في النموذج ونقصد به وعي الموظف باستخدام الأجهزة المحمولة **Laptop** فلا يشبك على شبكات واي فاي عامة ولا يتبث برمجيات مجهولة المصدر دون موافقة إدارة امن المعلومات، ولايستخدم وسائط تخزين محمولة دون فحصها من الإدارة المختصة وغير ذلك من الاحتياطات الواجبة. أشارت النتائج إلى أن الأجهزة المحمولة لها علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن الأجهزة المحمولة تعد مؤشرا هاما حيث أن زيادة فهم طريقة التعامل مع الأجهزة المحمولة يؤدي إلى زيادة مستوى أمن المعلومات بمقدار 0.65، وتشير القيمة **p=0.000**وهي أقل من 0.05 إلى نتائج ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 43% من التغير في المتغير التابع، وهو الوعي الأمني السيبراني، يمكن تفسيره أو يمكن التأثير عليه بواسطة المتغير المستقل، وهو استخدام الأجهزة المحمولة. مما يعني أن فهم الية التعامل مع الأجهزة المحمولة يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن الفرضية الثامنة لها تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

9. الفرضية التاسعة

معالجة المعلومات هو المتغير التاسع الذي تم اختباره في النموذج، ونقصد بمعالجة البيانات هي معرفة الموظف بكيفية معالجة المعلومات بطريقة سليمة بحيث لا يحدث تسريب لها ويطلع عليها غير المخولين ويتخلص من المطبوعات الزائدة دون أن يعرض معلومات المصرف أو خصوصية الزبائن للانتهاك. أشارت النتائج إلى أن وعي الموظف بآليات معالجة المعلومات له علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن الوعي بمعالجة المعلومات يعد مؤشرا هاما حيث أن زيادة فهم اليات معالجة المعلومات مع الوعي بأمن المعلومات يؤدي إلى زيادة أمن المعلومات بمقدار 0.41 ، وتشير القيمة **p=0.000** وهي أقل من 0.05 إلى نتائج ذات دلالة إحصائية، وقيمة معامل التحديد **(R Square)** يشير إلى أن 17% من التغير في المتغير التابع، وهو الوعي الأمني السيبراني، يمكن تفسيره أو يمكن التأثير عليه بواسطة المتغير المستقل، وهو معالجة المعلومات. مما يعني أن معالجة المعلومات يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن الفرضية التاسعة الذي يشير إلى أن معالجة المعلومات الموظفين تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات لدى عينة الدراسة.

10. الفرضية العاشرة

الإبلاغ عن الحادث هو المتغير العاشر الذي تم اختباره في النموذج، أشارت النتائج إلى أن الإبلاغ عن الحادث له علاقة إيجابية بالوعي بأمن المعلومات، ويشير النموذج إلى أن الإبلاغ عن الحادث يعد مؤشرا هاما حيث أن زيادة الإبلاغ عن الحادث مع الوعي بأمن المعلومات يؤدي إلى زيادة أمن المعلومات بمقدار 0.756، وتشير القيمة **p=0.000** وهي أقل من 0.05 إلى نتائج ذات دلالة إحصائية، قيمة معامل التحديد (**R Square**) يشير إلى أن 57% من التغير في المتغير التابع، وهو الوعي الأمني السيبراني، يمكن تفسيره أو يمكن التأثير عليه بواسطة المتغير المستقل وهو الإبلاغ عن الحادث. مما يعني أن الإبلاغ عن الحادث يعد مؤشرا هاما للوعي بأمن المعلومات، وبالتالي فإن **الفرضية العاشرة** الذي يشير إلى أن الإبلاغ عن الحادث الموظفين تجاه السياسات والإجراءات والبروتوكولات له تأثير إيجابي على الوعي بأمن المعلومات في المصارف الخاصة في مصراتة.

رابعاً/ توصيات الدراسة:

1. التوصيات

- ✓ نوصي بأن يتم وضع استراتيجية وطنية للأمن السيبراني للمصارف شاملة ومتكاملة، تركز على التحسين المستمر للوعي بأمن السيبراني للموظفين والعملاء، وتطوير القدرات الفنية والتكنولوجية.
- ✓ نوصي بأن تنشأ كل مؤسسة مصرفية سياسة خاصة بها للأمن السيبراني وتضع آلية للتدريب عليها ومن تم تنفيذها ووضع الية مراقبة ومتابعة وتحديث لها.
- ✓ نوصي بتعزيز التعاون مع الجهات المعنية والمؤسسات الأمنية الأخرى مثل الهيئة الوطنية لأمن وسلامة المعلومات والمراكز الأمنية لتبادل المعلومات والخبرات في مجال أمن المعلومات.
- ✓ نوصي بتطبيق المعايير الدولية لإدارة أمن المعلومات منها المعيار الدولي**ISO 27001** .
- ✓ نوصي بإنشاء إدارة او قسم خاص بأمن المعلومات في كل فرع أو مصرف وبناء القدرات الخاصة بهذا المجال. تهتم هذه الإدارة بتوفير التقنيات والحلول الفنية والاستجابة للمخاطر السيبرانية.

2. الدراسات المستقبلية

- ✓ نوصي بتطوير الدراسة بزيادة العينات المستهدفة لتشمل كافة المصارف التجارية العاملة.
- ✓ نوصي بإضافة مجالات تركيز أخرى لزيادة دقة النموذج وتوفير مقاييس أخرى لقياس الوعي بأمن المعلومات ولا تقتصر على 63 سؤال.
- ✓ نوصي بإعادة توزيع الاستبيان وبإجراء مقابلات شخصية مع الموظفين نفسهم بعد اجراء تدريب مكثف لهم لقياس مدى تحسن مستوى الوعي بأمن المعلومات لديهم.

المـــراجـــع

[1] نشوه إسماعيل زقوت و سناء أحمد السائح و الصديق عبد القادر العطاب 2022، مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية أمن المعلوماتفي ظل التحول الرقمي-دراسة تطبيقية بجامعة الزاوية للمجلة الدولية للعلوم والتقنية.

[2] Dharmawansa, A. D., & Madhuwanthi, R. A. M. 2020. Evaluating the Information Security Awareness (ISA) of employees in the banking sector: A case study. 13th International Research Conference General Sir John Kotelawala Defence University,2020.

[3] Osman, A. 2021. Cyber security awareness among employees of SMES In Libya. MSc. Thesis, Universiti Teknologi Malaysia.

[4] المركز العالمي لبناء القدرات السيبرانية أكسفورد 2023،تقرير فني، استعراض قدرات أمن المعلومات في ليبيا، الوصول اليه من الهيئة العامة للاتصالات والمعلوماتية، (غير منشور). المصدر الهيئة العامة للاتصالات والمعلوماتية، طرابلس.

[5] Stefaniuk, T. 2020. Training in shaping employee information security awareness. Entrepreneurship and Sustainability Issues, 7(3), 7 (3), 1832-1846, https://doi.org/10.9770/jesi.2020.7.3(26).

[6] Benqdara, S. 2023. Building an Information Security Awareness Program for a Private Financial Organization: Case from Libya. International Journal of Computer Applications, 975, 8887.

[7] Limna, P., Kraiwanit, T., & Siripipattanakul, S. 2023. The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. International Journal of Computing Sciences Research, 7, 1133-1151.

[8] Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. 2020. Machine learning approaches in cyber security analytics (pp. 37-200). Singapore: Springer.

[9] Tabachnick, B. G., & Fidell, L. S. 2013. Using multivariate statistics (6th ed.). Pearson. [8] Angelos P. Markopoulos. Finite Element Method in Machining Processes. Springer. 2013.

Information Security Awareness Among Employees of a Private Financial Organization: Case from Misurata, Libya

Ali A. Elrowayati
Dept. of Electronic Engineering, College of Industrial Technology, Misurata, Libya.
elrowayati@yahoo.com

Serajaldin M. Elsuwidi
Dept. of Electronic Engineering, College of Industrial Technology, Misurata, Libya.
serag.mustafa@cit.edu.ly

Abstract

Banks rely heavily on information security to safeguard their critical data and infrastructure. Because employees can be vulnerable to cyber threats, it's crucial to educate and train them to mitigate these risks. This study investigated information security awareness among Libyan bank employees in Misrata City using the Knowledge, Attitude, Behavior (KBA) model. It explored how knowledgeable employees are about information security and what factors influence their awareness. Researchers surveyed a group of employees using a questionnaire that assessed their knowledge, attitude, and behavior towards information security. The results revealed a positive correlation between employee awareness and the importance of information security. Interestingly, password management was the one area where employees showed a lack of awareness. The study recommends developing a national information security strategy for banks, alongside ongoing training programs for employees.

Keywords: Information security, Cybersecurity, Information security awareness, Information security policy.