مجلة جامعة فزان العلمية
Fezzan University scientific Journal
journal@fezzanu.edu.ly

دور الموظفين في تعزيز أو إضعاف أمن المعلومات بالمؤسسات: دراسة تحليلية في منطقة الجفرة

*مصباح ابوبكر مصباح[1]
[1]كلية تقنية المعلومات، جامعة الجفرة

الملخص

يشهد العالم تنافسا كبيرا بين مطوري برامج الحماية ولصوص البيانات؛ حيث تكونت علاقة طردية بينهما؛ كلما زادت وسائل الحماية سواء تقنية او سياسة ترتب عليها تطور في نوعية وطرق الاختراق واللصوصية، ولقد كان التطوير مرتكزا على الجانب التقني أكثر من غيره؛ حيث يوجد هنالك مكونا أساسيا في المنظمات يمكن أن يكون عنصرا مطورا أو يكون عنصرا مدمرا ومسببا في انهيار المؤسسة الذي يتمثل في الموظف؛ حيث يعتبر الموظف العنصر المذكور سابقا، فهو العنصر القائم على إدارة البيانات والمطلع على أسرار واستراتيجيات عمل المؤسسية ووسيلة المنظمة في تسيير دورة حياتها؛ فبإمكانه التسبب في خسائر كبيرة إما عن طريق ارتكاب الأخطاء جهلا أو عن طريق تعمد ارتكابها، أو عن طريق الجهل بسياسات الحماية المطبقة بالمؤسسة، وهذا ينتج من عدة عوامل منها الضغوط النفسية سواء عائلية، مجتمعية أو صرامة المتابعة والتشديد على انجاز العمل. من خلال هذه الورقة نقوم على دراسة مجموعة من الأبحاث المنشورة وتقارير المؤسسات المعنية بأمن المعلومات، ومحاولة المقاربة بين الآراء واستخلاص الأفعال التي يقوم بها الموظف التي تتسبب بخرق وسرقة وإتلاف معلومات المؤسسة في نقاط واستعمالها عبر استبيان لدراسة مدى انطباقها على مؤسسات منطقة الجفرة العامة منها والخاصة.

كلمات مفتاحية: الموظف وأمن المعلومات، أمن المعلومات بمنظمات الجفرة، حماية البيانات، سياسة أمن المعلومات، تدريب ومراقبة الموظفين.

"The Role of Employees in Strengthening or Weakening Information Security in Organizations: An Analytical Study in the Al-Jufrah Region"

* *Musbah Abubakr Musbah*[1]
[1]*Faculty of Information Technology, Waddan, University of Jufra*

Abstract

The world is witnessing intense competition between cybersecurity developers and data thieves, forming a direct relationship between them. As security measures, whether technical or policy-based, increase, the nature and methods of hacking and theft evolve accordingly. Development has primarily focused on the technical aspect more than others, as there is a fundamental component in organizations that can either be a driving force for progress or a destructive element leading to the collapse of the institution, and this is represented by the employee. The employee is the one who manages data, is aware of the secrets and strategies of the organization, and is the means through which the organization operates its lifecycle. The employee can cause

* المؤلف الرئيسي: عناوين البريد الإلكتروني musbah_7@hotmail.com

تاريخ استلام البحث 13 أبريل 2025 استلام رد المحكمين 30 ابريل 2025 تم قبوله 25 مايو 2025 تاريخ النشر 10 يونيو 2025

significant losses, either by making mistakes out of ignorance, intentionally committing them, or through ignorance of the security policies implemented within the institution. This ignorance may result from several factors, including psychological pressures, such as family and societal stress or the strict monitoring and pressure to accomplish tasks. Through this paper, we aim to study a collection of published research and reports from institutions concerned with information security, attempt to compare opinions, and extract actions performed by employees that lead to violations, theft, and destruction of organizational information. These actions will be summarized and examined through a survey to assess their applicability to both public and private institutions in the Al-Jufra region.

Keywords: *Employee and Information Security, Information Security in Organizations of Al-Jufra, Data Protection, Information Security Policy and Employee Training and Monitoring*

المقدمة:

غالبا ما تركزت الأبحاث حول انتهاك الموظفين لسياسات أمن المعلومات على عدم الامتثال بسبب ضعف التدريب وانخفاض تحفيز الموظفين، أو ضعف الالتزام الفعال، أو الرقابة الفردية. كما اتفقت أغلب الأبحاث المتخصصة في سلوك الموظف أو التزام الموظف بسياسات أمن المعلومات على أن " استخدام الإنترنت في المؤسسات أدى إلى جعل الموظفين أكثر كفاءة من خلال توفير قنوات اتصال محسنة، وأماكن عمل أفضل في تصميم الوظائف وظروف العمل من ناحية أخرى، أدى سوء استخدام الإنترنت في مكان العمل إلى حدوث بعض النكسات في المنظمة الناتجة عن فقدان نزاهة الشركة وتوافرها وسرية موارد النظام، وانخفاض أداء الموظفين، والمسؤولية القانونية، والكشف عن الأسرار التجارية، وغيرها من المخاوف الأمنية. ولقد كشف تقرير صادر عن شركة shred–it وهي إحدى الشركات المتخصصة في أمن المعلومات عن أكبر خطر يواجه الأمن الإلكتروني بالشركات هو إهمال الموظفين؛ حيث ورد بالتقرير أن 47% من قادة الأعمال اتفقوا على أن خطاء بشريا مثل الفقدان العرضي لجهاز أو مستند من قبل موظف تسبب في اختراق بيانات منظمتهم، هذا وقد تم استطلاع أكثر من 1000 من أصحاب الأعمال الصغيرة والمديرين التنفيذيين في الولايات المتحدة عبر الإنترنت في شهر ابريل /نيسان الماضي للحصول على التقرير [12]. وعلى لسان السيد "مونو كالسي" نائب رئيس شركة shrel–it " تظهر نتائج الدراسة بوضوح أن عادات الموظفين الصغيرة على ما يبدو يمكن أن تشكل مخاطر أمنية كبيرة على الشركات ". وفي عام 2017 كلفت عملية الاختراق لبيانات الشركة ما متوسطه 3.6 مليون دولار على مستوى العالم وفقا لتقرير منفصل صادر عن معهد بونيمون المتخصص في إجراء أبحاث حول الخصوصية وحماية البيانات وسياسة أمن المعلومات [12].في الحياة اليومية لكل فرد، أصبحت التقنيات متكاملة ومنتشرة في كل مكان دون إدراك ذلك، وأصبح المستخدم عرضة للهجوم السيبراني. ينجذب المتسللون الإجراميون لسرقة المعلومات الشخصية والتنظيمية. وبالتالي، يجب منع نقل بيانات الشركة إلى التطبيقات الشخصية سواء كانت الأجهزة شخصية أو شبكات الكمبيوتر. أما بالنسبة للتنظيم، فإن المعلومات والبيانات تعتبر ضرورية لخطة تنظيمهم وسلوكهم التجاري ونجاحهم المستقبل. [11]

يعد أمن المعلومات مصدر قلق دائم لجميع المنظمات. تتراوح التقديرات المالية لتأثير الخروقات الأمنية على موارد المعلومات والتكنولوجيا من مئات المليارات إلى أكثر من تريليون دولار سنويًا في جميع أنحاء العالم. [4] لذلك قامت المنظمات بتطوير مجموعة من الضوابط الفنية والإدارية والمادية للحد من هذه المخاطر. [3]

ولسوء الحظ، تم توثيق حالات عدم امتثال الموظفين المتعمد وغير المتعمد لسياسات أمن المعلومات، حيث خلص بعض خبراء الأمن إلى أن الموظفين هم الحلقة الأضعف في دفاعات أمن المعلومات. [2]

على الرغم من أن وسائل الإعلام الشعبية تميل إلى تناول مآثر المتسللين أو المتسللين، تشير الأدلة إلى أن غالبية حوادث أمن المعلومات تحدث نتيجة لتصرفات الموظفين الموثوق بهم.[9]

أكبر المخاوف في المنظمات لمديري أمن نظم المعلومات هي عندما تأتي تهديدات وهجمات أمن المعلومات من المطلعين على بواطن الأمور أو المعروفين على وجه التحديد بالعاملين أو العاملين داخل المنظمات. [10]

تعد المعلومات أحد الأصول التي توفر معاني قيمة للمنظمات نحو اتخاذ قرارات فعالة وفي المقابل إعطاء الربح للمنظمة. ومع ذلك، ينبغي أن تؤخذ حماية المعلومات القيمة التي تمثل أصولًا للشركات والمؤسسات على محمل الجد، حيث إن تقدم التقنيات ووسائل التواصل الاجتماعي وإنترنت الأشياء (IoT) في عصر المعلومات اليوم لا يوفر العديد من الفرص والمزايا لمشاركة المعلومات فحسب، بل يوفر أيضًا العديد من الفرص والمزايا لمشاركة المعلومات وأيضا التحديات التي تشمل مخاطر أمن المعلومات والخصوصية. [1]

1. العادات الأساسية السيئة للموظفين

اتفقت كل الأبحاث الواردة بجدول المراجع قيد الدراسة على ان الخروقات تحدث بسبب إما سلوكيات متعمدة، وهي نوع السلوك الذي يهدف إلى ارتكاب جرائم وتهديدات أمنية للأشخاص والمنظمات التي يمكن أن تسبب العديد من المشكلات الأمنية و التهديدات، أو سلوكيات غير متعمدة أو غير المسؤولة التي من المحتمل أن تجعل صاحبها عرضة للهجوم والتهديدات .

إن العديد من أخطر الجرائم التي يرتكبها الموظفون هي أشياء قد لا يفكرون أنها سلوك محفوف بالمخاطر، حيث اعترف أكثر من 25% من الموظفين الذين شملهم استطلاع Shred-It بأنهم تركوا حاسوبهم بدون قفل ودون رقابة. [12]

حتى تدوين الملاحظات على الورق، أو ترك الأوراق على مكتبك، قد يكون له عواقب غير مقصودة، فعندما تستخدم ورقة لتوثيق الملاحظات أو محضر الاجتماع فإنه من الخطر ترك هذه المعلومات في مكان يسهل الوصول إليه، فخطأ بسيط يمكن أن يأتي بنتائج عكسية. كما إن زيادة التواصل والتقدم التكنولوجي يعني أنه يمكن للموظفين العمل من أي مكان تقريبًا – قد يكون العمل من مقاهي أو حتى من غرفة المعيشة الخاصة بك لطيفًا ومريحًا، ولكنه قد يؤدي أيضًا إلى تعرض المؤسسة لاختراق بيانات خطير. لوحظ أيضا أن عمل الموظفين عن بعد آخذ في الازدياد بشكل كبير. حيث أن أكثر من نصف مديري التوظيف يوافقون على العمل عن بعد ويعتقدون أنه مستقبل العمل. هذا ويتفق معظم المسؤولين التنفيذيين على أن خطر حدوث اختراق للبيانات يكون أعلى عندما يعمل الموظف عن بعد، ولكن عدد قليل من الشركات لديها سياسات شاملة خارج الموقع متوفرة لهؤلاء الموظفين. في حين قال أكثر من نصف أصحاب الأعمال الصغيرة إنهم ليس لديهم سياسة للعاملين عن بعد. بالإضافة إلى ذلك، فإن المقاولين أو الموردين الخارجيين يفتحون أيضًا مجال لاختراقات البيانات في الشركات التي يتعاملون معها.

حيث وجد أن 1 من كل 4 مديرين تنفيذيين و1من كل 5 من أصحاب الأعمال الصغيرة قالوا إن البائع الخارجي كان السبب في اختراق البيانات في شركتهم ويرجع ذلك إلى أن العديد من الشركات لا تقوم بعمل مراجعة لصلاحيات الوصول للبيانات عندما تنتهي علاقتهم مع شركة خارجية، لذلك لابد أن يكون هناك تحكم أفضل وإدارة صحيحة لهذه الأمور.[12]

2. استخلاص عوامل الاتفاق .

مما سبق و من العديد من الأوراق والأدبيات المدرجة بقائمة المراجع تمكنا من استخلاص العادات السيئة التي تؤدي الى خرقا في نظام معلومات المؤسسة و التي يمكن أعتمدها كمقياس لأمن معلومات المؤسسات وهي كالتالي :-

أ . الإهمال و عدم المبالاة من قبل الموظف.

هذه النقطة منوطة بالدرجة الأولى بالموظف فان عدم إهنمامه بتنفيذ الإجراءات السليمة عند انجاز المهام المكلف به وإهماله لأي ملاحضات أو نتائج تنتج عن الإهمال في حد ذاته كارثة, فمثلا كماسبق الذكر أن تدوين الملاحظات على الورق، أو ترك الأوراق على المكتب، أو تستخدم ورقة لتوثيق الملاحظات أو محضر الاجتماع فإنه من الخطر ترك هذه المعلومات في مكان يسهل الوصول إليه وكما أن ترك الأجهزة عند نهاية الدوام مفتوحة أيضا قد يسبب خسائر في غناً عنها، أيضا ترك أشخاص غير مسؤولين وحدهم بالمكتب والخروج ولو لقضاء الحاجة دون اتخاد التدابير الأمنية.

ب . توفر إمكانية الوصول العشوائي.

هذه النقطة لها علاقة باتساع استخدام التكنلوجيا والإنترنت والتعامل الغير مباشر مع العملا عن بعد. فعملية الوصول لسلة معلومات المؤسسة من أي مكان يزيد من احتمالية وصول غير المعنيين ببيانات المؤوسسة " المخترقون و لصوص البيانات ".

فإن استخدام أجهزة غير موثوقة يمكن لمن له خبرة ولو بسيط في علم الحاسوب من خلالها تعقب كلمات المرور وعنوان سلة البيانات و إعادة استخدامها، ولا ننسى الهاتف المحمول في حل ضياعه أو سرقته يمكن استخدامه أيضا في اختراق امن المعلومات والوصول الي سلة البيانات للمؤسسة .

أ . عدم تطبيق سياسة صارمة للعمل عن بعد.

هذه النقطة هي أساس حدوث النقطتين السابقتين؛ فإن خطر حدوث اختراق للبيانات يكون أعلى عندما يعمل الموظف عن بعد، في حال ليس لديها سياسات شاملة خارج الموقع متوفرة لهؤلاء الموظفين و العملاء .

ب . عدم توافر سياسة صارمة للعمل الداخلى و العمل المباشر مع العملاء.

هذه النقطة قد تكون سببا للخرق؛ ففي حال عدم وجود ظوابط فان النقاط السابقة سوف تحدث مع مرور الوقت فمثلا عند استقبال العملاء في المكتب فانه قد يرى أشياء لا يجب أن يراها كما سبق دكره في النقطة الأولى "الإهمال و عدم المبالاة

3. منهجية إعداد الاستبيان

تم تصميم الاستبيان على المعلومات المجمعة من الاستخلاص السابق حول السلوكيات المؤدية لخرق البيانات سواء كانت متعمدة او عفوية، وتم استخدام الذكاء الاصطناعي في التأكد من دقة الاستبيان وتناسبه مع النقاط المستخلصة، وكما تم استهداف المدراء العامون و المدراء المكاتب بعدد 50 مؤسسة منها 31 مؤسسة عامة و 19 مؤسسات خاصة فقط؛ وهذا لصغر المنطقة المستهدفة بالدراسة، واعتذارعدد كبير من المؤسسات عن إجابة الاستبيان ، كما تم استهداف مدراء المؤسسات بهذا الاستبيان عبر مقابلة استغرقت نصف ساعة لكل مؤسسة .

للاطلاع على الاستبيان انظر للملحق .

و تلخص الاستبيان على النقاط التالية و المستخلصة من الفقرة السابقة :

1 . مدى معرفة الموظف بسياسة حماية البيانات .

2 . مدى معرفة الموظف بعواقب الإهمال بحماية البيانات .

3 . مدى استخدام الانترنت بالعمل .

4 مدى متابعة الصلاحيات الممنوحة للعملاء للولوج ألى بيانات المنظمة .

5 . طريقة التعامل مع العملاء ونوعها .

6 . مدي استعمال النقال في ارسال واستقبال و التعامل مع العملاء عن بعد.

7 . حدود استعمال النقال .

8 . مدى التزام الموظفين بحماية معلومات المنظمة .

هذه النقاط تمثل اهم النقاط التي يمكن للموظف منها بالتسبب بثغرة امنية تؤدي الى خسارة قيمة مالية كبيرة جدا , كما انها الباب الذي يمكن للموظف احداث خلل متعمد من خلالها .

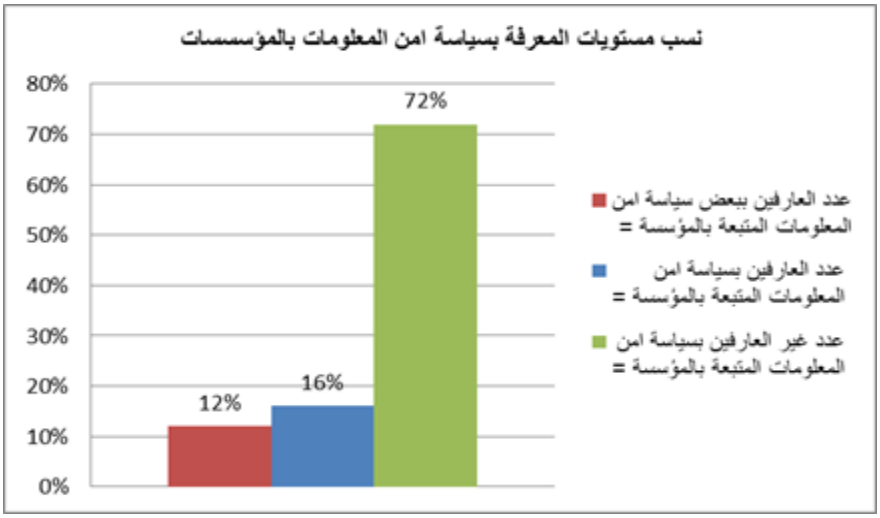
4. تحليل البيانات

الشكل (1) الذي يبين توزيع المؤسسات بين كبيرة وصغيرة ومتوسط و الحكومية منها والخاصة .

الشكل(1) توزيع المؤسسات حسب الحجم و التصنيف

A .الوعي الأمني للموظفين

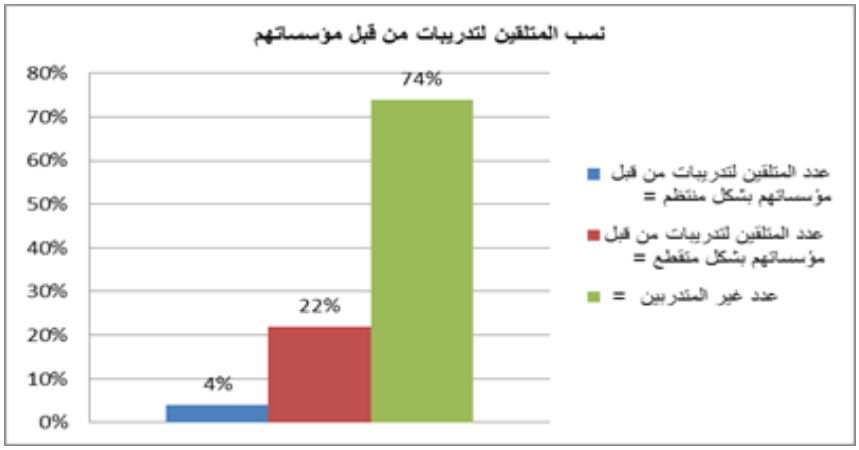
من خلال الشكل (2) و المستنتج من إجابات السؤال العاشر نجد أن عدد العارفين بسياسة أمن معلومات المؤسسة التابعين لها نسبة ضعيفة جدا وهي تقدر بـ 16% من إجمالية المستبانين الذي بلغ عددهم كما ذكرنا 50 شخصا



الشكل(2) نسب مستويات المعرفة بامن المعلومات بالمؤسسات

والبقية منقسمون بين عارف ببعض السياسات وتحديدا الواضحة منها؛ كمنع دخول غير العاملين للمكتب وإطفاء الجهاز عند الخروج من العمل، ووجوب وجود مضاد للفيروسات مثلا . وهذه المجموعة لا تتعدى 12% أما الغالبية العظمى التي تقدر ب 72% لا يملكون أدنى معرفة بما معناه سياسة أمن المعلومات .

ومن خلال الشكل(3) لإجابة السؤال الحادي عشر الذي له علاقة بالتدريب على سياسة الحماية .

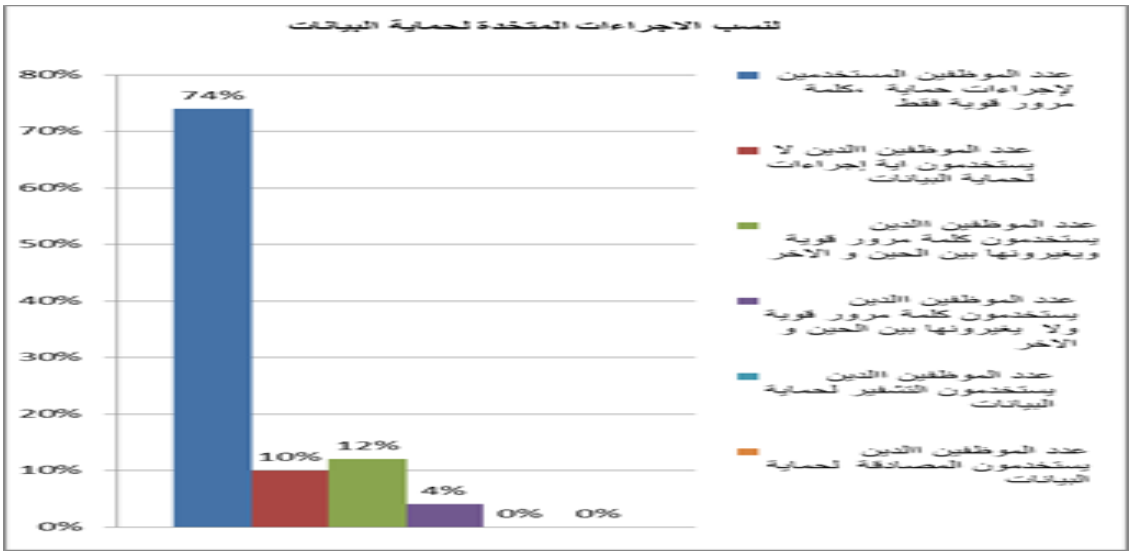


الشكل (4) نسب المتلقين للتدريبات من قبل مؤسساتهم

نجد أنه يوجد تقارب في الإجابات كبير جدا , فنسبة غير المتدربين 74% في حين 72% منهم هم الغير عارفين بسياسة مؤسساتهم , اما البقية فمنقسمين الى صنفين صنف منتظم في تلقي الدورات التدريبية والقسم الآخر لا يتلقى تدريبا منتظما . ومن هذا نجد أن الوعي الأمني للموظفين مرتبط بمدى معرفة الموظف بسياسة المؤسسة في أمن المعلومات، كما أن المنطقة تعاني نقصا في الاهتمام بتوعية موظفيها وتدريبهم على كيفية العمل على خلق بيئة عمل آمنة .

a . السلوكيات الأمنية للموظفين

في السؤال الثاني عشر من الاستبيان الذي يتحدث فيه عن نوع الإجراءات المتبعة من قبل المستبان لحماية البيانات التي يتعامل معها من استخدام لكلمة مرور قوية أو تغير كلمة المرور بانتظام او استخدام عملية المصادقة أو التشفير أو أنه لا يتخذ أي إجراء منها , كانت الإجابات صادمة فمن الشكل (5) نجد أن ما نسبته 74% يعتقدون أن كلمة المرور القوية هي تأمين للبيانات وأنهم لا يستخدمون أي شيء آخر، اما العارفون بماهية أمن المعلومات فهم من يستخدمون كلمة مرور قوية، ويحرصون على تغييرها دوريا، وهم لا يتعدون 12% وهي نسبة مساوية لنسبة العارفين بأمن المعلومات التي ذكرناها سابقا، وهذا إن دل فإنه يدل على دور المعرفة بأمن المعلومات في اتخاذ الإجراء المناسب .

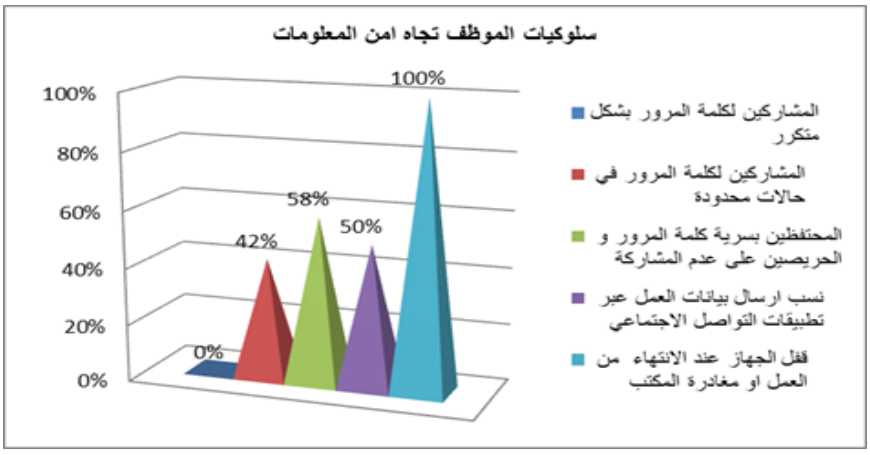


الشكل (5) توزيع الإجراءات المتبعة لحماية البيانات

اما ما نسبته 4% فهم عارفون مقتنعون بمبداء تجديد كلمة المرور، ولكنهم لا يفعلون ذلك، ومعتمدون فقط على كلمة سر قوية يصعب اختراقها، هذا يعد عدم حرص منهم .

كما أن نسبة استخدام التشفير والمصادقة غير موجودة فهي 0% لكلاهما، كما قمت بمراجعة بعض الشركات والمؤسسات حول عدم استخدامهم لهده التقنيات؛ فتم التبرير بعدم وجود تقنية عالية لديهم، وأن أغلبهم يستعمل مواقع التواصل الاجتماعي, كما أن اغلبهم لديه جهل بمعنى التشفير والمصادقة

ونجد في نتيجة السؤال الخامس عشر والسادس عشر واللذان يشيران لإهمال وعدم مبالا من قبل الموظفين؛ فما نسبته 100% أو كل الإجابات كانت تعبيرا عن حرص الموظف على سلامة البيانات باغلاق الجهاز عند المغادرة، كما أن الشكل (6) الذي يوضح قياسا لسلوك الموظفين من عدم مشاركة كلمة المرور مع آخرين .

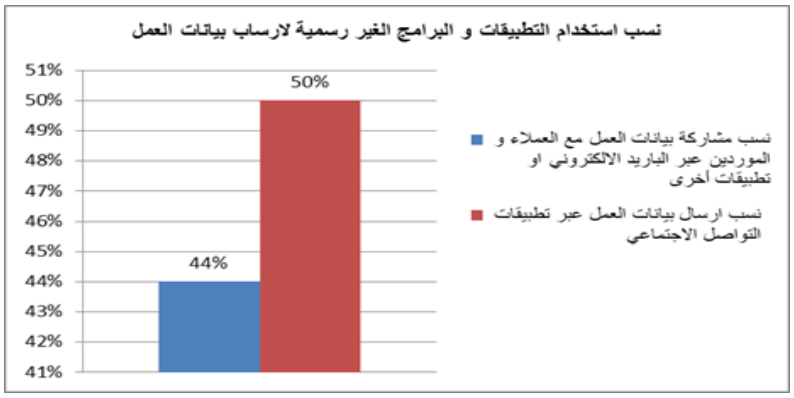


الشكل(6) سلوكيات الموظف تجاه امن المعلومات

a. الثغرات الأمنية المحتملة

من خلال السؤال الثامن توصلنا إلى أن مانسبته 100% من الموظفين يستخدمون أجهزة غير أجهزة العمل في تبادل البيانات وعند المناقشة معهم تبين أن مانسبته 50% يستخدمون الأجهزة المحمولة الخاصة؛ وذلك من خلال

منصات التواصل الاجتماعي؛ مع اعتقادهم بأن هذا الاستخدام يسرع العمل. وهذا ماثبت معنا بالإجابة للسؤال الثامن عشر عبر الشكل (7) حيث كانت نسبة 50% من الموظفين يتبادلون بيانات العمل عبر منصات التواصل الاجتماعي؛ مما يوسع الاحتمال لتسريب واختراق البيانات .



الشكل (7) نسب استخدام الأجهزة والتطبيقات الغير رسمية

من خلال السؤال الخامس والعشرون اتفق الجميع على أن نقص التدريب عامل أساسي في أمن معلومات المؤسسة ولكن الباحث يرى أن هناك عوامل كثير منها الجهل بمهية سياسة المعلومات، و تحديد سياسة العمل من حيث الممنوعات أو المحضورات كاستخدام أجهزة غير المخصصة للعمل، والعمل خارج أوقات الدوام و غيرها حيث يجب تحديد المسارات و تدريب الموظفين و من ثم إعلامهم بالعواقب المترتبة على الإهمال أو تعمد خرق سياسة العمل و أمن المعلومات .

5. النتائج

ركزت هذه الورقة البحثية على دور الموظف في تحقيق أو إضعاف أمن معلومات المؤسسة، مع تسليط الضوء على العلاقة المتنامية بين تطور تقنيات الحماية وابتكار أساليب الاختراق. توضح الدراسة أن الموظف، كعنصر رئيسي في إدارة البيانات والاطلاع على أسرار المؤسسة، قد يكون سبباً في خسائر جسيمة سواء عن عمد أو نتيجة للجهل بسياسات أمن المعلومات.

استندت الدراسة إلى مراجعة مجموعة من الأبحاث والتقارير العالمية والمحلية، واستخدمت استبياناً شمل 50 مؤسسة بمنطقة الجفرة (منها عامة وخاصة) لتقييم مدى معرفة الموظفين بسياسات الحماية وإتباعهم للإجراءات الأمنية. وأسفرت النتائج عن:

أ . ضعف الوعي بسياسات أمن المعلومات حيث أفاد 72% من المشاركين بعدم امتلاكهم المعرفة الكافية.

ب . نقص التدريب الفعّال , إذ لم يتلقَ غالبية الموظفين التدريب المنتظم حول أمن المعلومات.

ج . اعتماد مفرط على أساليب حماية بسيطة مثل كلمة المرور القوية، مع غياب استخدام تقنيات إضافية كالمصادقة الثنائية والتشفير.

د . انتشار استخدام الأجهزة الشخصية وتبادل البيانات عبر تطبيقات التواصل الاجتماعي، مما يزيد من مخاطر التسريب والاختراق.

التوصيات

أ . تعزيز برامج التدريب والتوعية:

تنظيم دورات وورش عمل دورية لتثقيف الموظفين بسياسات أمن المعلومات وإبراز تأثير سلوكياتهم على سلامة بيانات المؤسسة.

ب . تفعيل سياسات صارمة لاستخدام الأجهزة والتطبيقات:

وضع قواعد واضحة تمنع استخدام الأجهزة الشخصية وتطبيقات التواصل الاجتماعي في تبادل البيانات الحساسة، مع توفير أجهزة مخصصة للعمل.

ج . اعتماد إجراءات تقنية متقدمة:

تفعيل تقنيات الحماية الإضافية مثل المصادقة الثنائية وتشفير البيانات لضمان أمان المعلومات وتقليل فرص الاختراق.

د . مراجعة وتحديث صلاحيات الوصول:

إجراء تدقيق دوري لصلاحيات الموظفين ومراجعة الإجراءات الأمنية بما يتماشى مع التغيرات التقنية ومتطلبات السوق.

هـ . تعزيز الرقابة والمتابعة:

تطبيق أنظمة رقابية تراقب سلوك الموظفين وتعزز من مساءلتهم عند مخالفة سياسات الأمن، مع وضع آليات للتبليغ عن المخالفات.

و . بناء ثقافة مؤسسية للأمن:

تشجيع بيئة عمل تحفّز على الالتزام بالأمن السيبراني من خلال إشراك الموظفين في وضع السياسات وتقديم الحوافز للممارسات الجيدة في مجال حماية المعلومات.ُعد هذه التوصيات خطوة أساسية نحو تقليل الثغرات الأمنية الناتجة عن سلوكيات الموظفين وتعزيز مستوى الأمان العام في المؤسسات، مما يساهم في حماية الأصول المعلوماتية وتقليل الخسائر المالية المحتملة.

5 . قائمة المراجع

[1] Alshare, Lane and Lane, (2018)Information security policy compliance: a higher education case study. Information and Computer Security, 00–00. https://doi.org/10.1108/ICS-09-2016-0073.

[2] Aurigemma, S., and Panko, R. (2012). A composite framework for behavioral compliance with information security policies. 45th Hawaii International Conference on Systems Sciences, IEEE Computer Society, Hawaii, 3248-3257.

[3] D'Arcy, J., and Herath, T. (2011a). A review and analysis of deterrence theory in the IS literature: making sense of disparate findings. European Journal of Information Systems, 20, 643-658 .

[4] D'Arcy, J., and Herath, T. (2011b). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.

[5] David, Sikolia., Marlys, J., Mason., David, P., Biros., Mark, Weiser. (2014). A Theory of Employee Compliance with Information Security.

[6] David, Sikolia. (2013). A Thematic Review of User Compliance with Information Security Policies Literature .

[7] Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee

[8] Jeffrey, M., Stanton., Kathryn, R., Stam. (2006). The Visible Employee:

[9] Karjalainen, M., and Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) Security training approaches. Journal of the Association for Information Systems, 12(8), 518-555.
[10] Li, Y. 2015. Users' information systems (IS) security behavior in different contexts.
[11] Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. International Journal of Academic Research in Business and Social Sciences, 9(6), 560–571.
[12] Mono Kalsi. 2019.Vice President of SHREL-IT Company, Times Of India Magazine (2019).
[13] O., A., Hoppe., J., F., van, Niekerk., Rossouw, von, Solms. (2002). The Effective Implementation of Information Security in Organizations. 1-18. Available from: 10.1007/978-0-387-35586-3_1
[14] N. S. Safa and R. von Solms, "Human Aspects of Information Security: A Behavioral Framework for Employee Security Compliance," Information & Computer Security, vol. 30, no. 2, pp. 195–211, 2022.
[15] A. Alqahtani, J. Al-Muhtadi, and A. Alshamrani, "Analyzing the Impact of Human Factors on Cybersecurity in Organizations," Journal of Information Security and Applications, vol. 59, pp. 102875, 2021.
[16] P. Ifinedo, "Understanding the Role of Employee Awareness and Attitudes in Preventing Cyber Threats," Computers & Security, vol. 125, pp. 102965, 2023.
[17] L. Hadlington and K. Parsons, "The Role of Human Error in Organizational Cybersecurity Breaches: A Meta-Analysis," Cyberpsychology, Behavior, and Social Networking, vol. 23, no. 3, pp. 184–190, 2020.
[18] A. Bada, A. Sasse, and J. Nurse, "Cybersecurity Awareness Campaigns: Why Do They Fail to Change Behavior?" Journal of Cybersecurity, vol. 8, no. 1, pp. 1–12, 2022.
[19] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements, 3rd ed., ISO, Geneva, Switzerland, 2022.
[20] National Institute of Standards and Technology (NIST), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST SP 800-46 Rev.3, 2023.

5. الملحق

استبيان لغرض الدراسة

يهدف هذا الاستبيان إلى دراسة سلوك الموظفين تجاه أمن المعلومات في المؤسسات، وذلك لتحديد العوامل التي تؤثر على التزامهم بسياسات الحماية وتحديد الثغرات الأمنية المحتملة. سيتم استخدام البيانات المجمعة لتحسين سياسات أمن المعلومات وتقديم توصيات لتعزيز الوعي الأمني لدى الموظفين.

القسم الأول: معلومات عامة

1. نوع المؤسسة :
   - حكومية ( )
   - خاصة ( )
2. حجم المؤسسة :
   - كبيرة ( )

- متوسطة ( )
- صغيرة ( )

3. ما هو دورك الوظيفي في المؤسسة؟

- مدير عام ( )
- مدير قسم ( )
- موظف إداري ( )
- موظف فني ( )
- أخرى _____ ( )

4. ما هي طبيعة عملك؟

- عمل مكتبي ( )
- عمل ميداني ( )
- عمل عن بعد ( )
- أخرى _____ ( )

القسم الثاني: استخدام التكنولوجيا والإنترنت

5. ما مدى اعتماد المؤسسة على التكنولوجيا في إنجاز المهام؟

- اعتماد كلي ( )
- اعتماد جزئي ( )
- اعتماد ضعيف ( )

6. ما مدى استخدامك للإنترنت في العمل؟

- بشكل يومي ومكثف ( )
- بشكل متقطع ( )
- نادرًا ( )
- لا أستخدم الإنترنت ( )

7. ما هي الأجهزة التي تستخدمها في العمل؟ (يمكن اختيار أكثر من خيار)

- جهاز كمبيوتر مكتبي ( )
- جهاز كمبيوتر محمول ( )
- هاتف ذكي ( )
- جهاز لوحي ( )
- أخرى _____ ( )

8. هل تستخدم أجهزة شخصية (غير تابعة للمؤسسة) في العمل؟

- نعم ( )
- لا ( )

9. ما هي التطبيقات أو البرامج التي تستخدمها بشكل متكرر في العمل؟

- البريد الإلكتروني ( )
- برامج التواصل الداخلي ( )
- برامج إدارة المهام ( )
- برامج التخزين السحابي ( )
- أخرى _____ ( )

القسم الثالث: الوعي الأمني وسياسات الحماية

10. هل تعرف سياسات أمن المعلومات المتبعة في المؤسسة؟
- نعم، أعرفها جيدًا ( )
- أعرف بعضها ( )
- لا أعرفها ( )

11. هل تلقيت تدريبًا على أمن المعلومات من قبل المؤسسة؟
- نعم، بشكل منتظم ( )
- نعم، ولكن بشكل محدود ( )
- لا، لم أتلق أي تدريب ( )

12. ما هي الإجراءات التي تتخذها لحماية البيانات التي تتعامل معها؟ (يمكن اختيار أكثر من خيار)
- استخدام كلمات مرور قوية ( )
- تغيير كلمات المرور بانتظام ( )
- استخدام المصادقة الثنائية ( )
- تشفير الملفات الحساسة ( )
- لا أتخذ أي إجراءات خاصة ( )

13. هل تعتقد أن سياسات أمن المعلومات الحالية في المؤسسة كافية؟
- نعم، كافية تمامًا ( )
- إلى حد ما ( )
- لا، غير كافية ( )

14. هل تعرضت لاختراق أو تسريب بيانات أثناء عملك؟
- نعم ( )
- لا ( )
- لست متأكدًا ( )

القسم الرابع: سلوكيات الموظفين تجاه أمن المعلومات

15. هل تقوم بقفل جهاز الكمبيوتر أو الهاتف عند مغادرة مكتبك؟
- دائمًا ( )
- أحيانًا ( )
- نادرًا ( )

- لا أقوم بذلك ( )

16. هل تقوم بمشاركة كلمات المرور أو بيانات الدخول مع زملائك؟

- نعم، بشكل متكرر ( )
- نعم، ولكن في حالات محدودة ( )
- لا، أبدًا ( )

17. هل تقوم بحفظ البيانات الحساسة على أجهزة شخصية أو وسائط تخزين خارجية؟

- نعم ( )
- لا ( )

18. هل تقوم بإرسال بيانات العمل عبر تطبيقات التواصل الشخصية (مثل واتساب، فيسبوك ماسنجر)؟

- نعم ( )
- لا ( )

19. هل تقوم بحذف البيانات المؤقتة أو غير الضرورية من الأجهزة التي تستخدمها؟

- دائمًا ( )
- أحيانًا ( )
- نادرًا ( )
- لا أقوم بذلك ( )

20. هل تعتقد أن سلوكياتك الشخصية قد تشكل خطرًا على أمن معلومات المؤسسة؟

- نعم ( )
- لا ( )
- لست متأكدًا ( )

القسم الخامس: العمل عن بعد والتعامل مع العملاء

21. هل تعمل عن بعد؟

- نعم، بشكل دائم ( )
- نعم، ولكن بشكل جزئي ( )
- لا، أعمل من المكتب فقط ( )

22. ما هي الإجراءات التي تتخذها لحماية البيانات عند العمل عن بعد؟ (يمكن اختيار أكثر من خيار)

- استخدام شبكات VPN ( )
- تجنب استخدام شبكات Wi-Fi العامة ( )
- استخدام أجهزة موثوقة فقط ( )
- لا أتخذ أي إجراءات خاصة ( )

23. هل تقوم بمشاركة بيانات العمل مع العملاء أو الموردين عبر البريد الإلكتروني أو التطبيقات الأخرى؟

- نعم ( )
- لا ( )

24. هل تقوم بمراجعة صلاحيات الوصول للعملاء أو الموردين بعد انتهاء العلاقة معهم؟

- نعم، دائمًا ( )
- أحيانًا ( )
- لا ( )

القسم السادس: التحديات والمقترحات

25. ما هي أكبر التحديات التي تواجهها في الالتزام بسياسات أمن المعلومات؟

- نقص التدريب ( )
- صعوبة تطبيق السياسات ( )
- ضغط العمل ( )
- عدم وجود حوافز للالتزام ( )
- أخرى _____ ( )

26. ما هي اقتراحاتك لتحسين أمن المعلومات في المؤسسة؟

شكرًا لوقتك ومشاركتك!