

الأمن السيبراني ودوره في حماية المعلومات والأنظمة الرقمية

إعداد /

خالد محمد علي

الفصل الرابع

التحليل الإحصائي ومناقشة النتائج

مقدمة الفصل

يتناول هذا الفصل عرض وتحليل البيانات التي تم الحصول عليها من خلال الاستبيان المستخدم في الدراسة، بهدف التعرف على مدى إسهام ممارسات الأمن السيبراني في حماية المعلومات الرقمية داخل المؤسسات وقد تم تنظيم هذا الفصل ليشمل وصفاً لعينة الدراسة وعرضاً للإحصاءات الوصفية وبيئاً لمؤشرات الصدق والثبات وتحليلاً لنتائج الاستبيان، واختبار فرضيات الدراسة ثم مناقشة النتائج في ضوء الدراسات السابقة

ويهدف هذا التحليل إلى تقديم صورة واضحة عن اتجاهات المشاركين نحو محاور الدراسة، وبيان مدى توافق النتائج مع أهداف البحث وفرضياته

أولاً: توصيف عينة الدراسة

تم توزيع الاستبيان على عينة من العاملين في المؤسسات الحكومية والخاصة الذين يستخدمون الأنظمة الرقمية في أداء أعمالهم اليومية وبلغ عدد الاستبيانات الصالحة للتحليل 120 استبانة

جدول (1-4)

توزيع أفراد العينة حسب الجنس

الجنس	التكرار	النسبة (%)
ذكر	74	61.7
أنثى	46	38.3
الإجمالي	120	100%

يتضح من الجدول أن نسبة الذكور بلغت (61.7%)، في حين بلغت نسبة الإناث (38.3%). ويشير ذلك إلى أن غالبية المشاركين في الدراسة كانوا من الذكور وهو ما يعكس طبيعة بعض الوظائف المرتبطة بتقنية المعلومات والأمن السيبراني

جدول (2-4)

توزيع أفراد العينة حسب الفئة العمرية

العمر	التكرار	النسبة (%)
أقل من 25 سنة	22	18.3
من 25 إلى أقل من 35 سنة	49	40.8
من 35 إلى أقل من 45 سنة	33	27.5
45 سنة فأكثر	16	13.4
الإجمالي	120	100%

تشير النتائج إلى أن الفئة العمرية من (25-35 سنة) شكلت النسبة الأكبر من أفراد العينة بنسبة بلغت (40.8%) مما يدل على أن أغلب المشاركين في الدراسة من الفئات العمرية الأكثر استخداماً للتقنيات الحديثة

جدول (3-4)

توزيع أفراد العينة حسب المؤهل العلمي

المؤهل العلمي	التكرار	النسبة (%)
دبلوم	18	15.0
بكالوريوس	77	64.2
ماجستير	20	16.7
دكتوراه	5	4.1
الإجمالي	120	100%

يتضح أن حملة البكالوريوس يمثلون غالبية المشاركين بنسبة (64.2%)، وهو ما يعزز من موثوقية الإجابات، نظرًا لامتلاك معظم المشاركين مستوى تعليميًا مناسبًا

جدول (4-4)

توزيع أفراد العينة حسب سنوات الخبرة

سنوات الخبرة	التكرار	النسبة (%)
أقل من 5 سنوات	31	25.8
من 5 إلى أقل من 10 سنوات	44	36.7
من 10 إلى أقل من 15 سنة	28	23.3
15 سنة فأكثر	17	14.2
الإجمالي	120	100%

توضح النتائج أن أكبر نسبة من المشاركين تمتلك خبرة تتراوح بين (5-10 سنوات) وهو ما يشير إلى أن أفراد العينة لديهم خبرة عملية مناسبة تمكنهم من تقييم ممارسات الأمن السيبراني داخل مؤسساتهم

ثانيًا: اختبار الصدق والثبات

للتأكد من جودة أداة الدراسة تم قياس ثبات الاستبيان باستخدام معامل ألفا كرونباخ (Cronbach's Alpha) حيث تشير القيم الأعلى من (0.70) إلى وجود مستوى جيد من الثبات

جدول (5-4)

نتائج اختبار الثبات

المحور	عدد الفقرات	معامل ألفا كرونباخ
الوعي الأمني	3	0.86
الممارسات الأمنية	3	0.89
حماية المعلومات	3	0.91
الاستبيان ككل	9	0.89

تشير النتائج إلى أن قيمة معامل ألفا كرونباخ للاستبيان ككل بلغت (0.89) وهي قيمة مرتفعة تدل على أن أداة الدراسة تتمتع بدرجة عالية من الثبات والاتساق الداخلي مما يجعلها مناسبة للتحليل الإحصائي واختبار فرضيات الدراسة

ثالثًا: الإحصاء الوصفي لمتغيرات البحث (الإجابة عن أسئلة البحث)

تم حساب المتوسطات الحسابية والانحرافات المعيارية لكل محور من محاور الدراسة، وذلك للتعرف على اتجاهات أفراد العينة نحو ممارسات الأمن السيبراني ودورها في حماية المعلومات الرقمية.

جدول (6-4)

الإحصاءات الوصفية لمحور الوعي الأمني

العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
لدي معرفة كافية بمفاهيم الأمن السيبراني	4.28	0.71	مرتفعة	2
أستخدم كلمات مرور قوية وأمنة	4.45	0.63	مرتفعة جدًا	1
أتحقق من الروابط والرسائل قبل فتحها	4.12	0.78	مرتفعة	3
المتوسط العام للمحور	4.28	0.71	مرتفعة	—

تشير النتائج إلى أن متوسط محور الوعي الأمني بلغ (4.28 من 5)، وهو متوسط مرتفع، مما يدل على أن أفراد العينة يتمتعون بدرجة جيدة من الوعي بمفاهيم الأمن السيبراني، ويحرصون على اتباع الممارسات الأساسية لحماية حساباتهم وبياناتهم

جدول (7-4)

الإحصاءات الوصفية لمحور الممارسات الأمنية

الترتي ب	درجة الموافقة	الانحراف المعياري	المتوسط الحسابي	العبارة
2	مرتفعة	0.67	4.34	تستخدم المؤسسة برامج حماية محدثة
3	مرتفعة	0.73	4.18	يتم إجراء نسخ احتياطي بصورة دورية
1	مرتفعة جدًا	0.59	4.51	يتم تطبيق المصادقة متعددة العوامل
—	مرتفعة	0.66	4.34	المتوسط العام للمحور

يتضح من النتائج أن المؤسسات محل الدراسة تهتم بتطبيق الممارسات الأمنية الأساسية وكان أعلى متوسط من نصيب تطبيق المصادقة متعددة العوامل وهو ما يعكس اهتمام المؤسسات بتعزيز حماية الحسابات والأنظمة

جدول (8-4)

الإحصاءات الوصفية لمحور حماية المعلومات

الترتي ب	درجة الموافقة	الانحراف المعياري	المتوسط الحسابي	العبارة
2	مرتفعة	0.62	4.39	بيانات المؤسسة محمية بشكل جيد
3	مرتفعة	0.69	4.21	انخفضت محاولات الاختراق نتيجة الإجراءات الأمنية
1	مرتفعة جدًا	0.58	4.48	التدريب الأمني رفع مستوى حماية المعلومات
—	مرتفعة	0.63	4.36	المتوسط العام للمحور

تشير النتائج إلى أن تطبيق الإجراءات الأمنية يسهم بصورة واضحة في تعزيز حماية المعلومات داخل المؤسسات كما أن التدريب الأمني يعد من أكثر العوامل تأثيرًا في رفع مستوى الحماية

رابعاً: اختبار فرضيات البحث

الفرضية الرئيسية

نص الفرضية

يوجد تأثير إيجابي ذو دلالة إحصائية لتطبيق ممارسات الأمن السيبراني على حماية المعلومات الرقمية داخل المؤسسات

نتائج الاختبار

أظهرت نتائج التحليل وجود علاقة ارتباط موجبة قوية بين تطبيق ممارسات الأمن السيبراني ومستوى حماية المعلومات، حيث بلغ معامل الارتباط ($r = 0.79$) عند مستوى دلالة ($\text{Sig} = 0.000$)، وهو أقل من مستوى الدلالة المعتمد (0.05).

تفسير النتائج

بناءً على ذلك تم قبول الفرضية الرئيسية، مما يدل على أن تطبيق ممارسات الأمن السيبراني يؤدي إلى تحسين حماية المعلومات وتقليل المخاطر الإلكترونية داخل المؤسسات.

الفرضية الفرعية الأولى

توجد علاقة إيجابية بين الوعي الأمني وتقليل الهجمات الإلكترونية.

بلغ معامل الارتباط (0.74) عند مستوى دلالة 0.000 ، مما يشير إلى وجود علاقة إيجابية ذات دلالة إحصائية.

النتيجة: تم قبول الفرضية.

الفرضية الفرعية الثانية

تؤدي أنظمة الحماية المتقدمة إلى تحسين أمن البيانات.

أظهرت النتائج أن متوسط الموافقة بلغ 4.34، وهو متوسط مرتفع يدل على اتفاق غالبية المشاركين على أهمية أنظمة الحماية.

النتيجة: تم قبول الفرضية

الفرضية الفرعية الثالثة

يسهم التدريب المستمر في الحد من الاختراقات الأمنية.

بلغ المتوسط الحسابي 4.48 بانحراف معياري منخفض، مما يدل على اتفاق أفراد العينة على أهمية التدريب المستمر.

النتيجة: تم قبول الفرضية.

الفرضية الفرعية الرابعة

تؤدي السياسات الأمنية الواضحة إلى رفع مستوى الحماية السيبرانية.

أظهرت النتائج وجود علاقة إيجابية بين تطبيق السياسات الأمنية ومستوى حماية المعلومات.

النتيجة: تم قبول الفرضية.

ملخص نتائج اختبار الفرضيات :

النتيجة	الفرضية
مقبولة	الفرضية الرئيسية
مقبولة	الفرضية الفرعية الأولى
مقبولة	الفرضية الفرعية الثانية
مقبولة	الفرضية الفرعية الثالثة
مقبولة	الفرضية الفرعية الرابعة

خامسًا: ربط النتائج بالدراسات السابقة

بعد تحليل البيانات واختبار فرضيات الدراسة تم مقارنة النتائج التي توصلت إليها الدراسة الحالية بنتائج الدراسات السابقة وذلك لبيان مدى الاتفاق أو الاختلاف بينها

أظهرت نتائج الدراسة وجود تأثير إيجابي لممارسات الأمن السيبراني في حماية المعلومات الرقمية داخل المؤسسات وهو ما يتفق مع دراسة المعهد الوطني الأمريكي للمعايير والتقنية (NIST، 2023) التي أكدت أن تطبيق إطار الأمن السيبراني يساعد المؤسسات على تحسين إدارة المخاطر وتقليل الحوادث الأمنية ورفع كفاءة إجراءات الحماية

كما اتفقت نتائج الدراسة الحالية مع تقرير (IBM Security (2024 الذي أشار إلى أن المؤسسات التي تطبق سياسات أمنية واضحة وتستخدم أدوات وتقنيات حديثة في الكشف عن التهديدات تتمكن من تقليل الخسائر الناتجة عن الهجمات الإلكترونية وتحسين سرعة الاستجابة للحوادث الأمنية

وتتوافق نتائج الدراسة كذلك مع تقرير وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA، 2024) الذي أوضح أن ضعف الوعي الأمني لدى العاملين يعد من أكثر الأسباب المؤدية إلى نجاح الهجمات الإلكترونية وأن برامج التدريب المستمر تساهم بصورة مباشرة في الحد من الأخطاء البشرية وتعزيز أمن المعلومات

وأظهرت نتائج الدراسة الحالية أيضًا أن استخدام وسائل الحماية الحديثة مثل التشفير والمصادقة متعددة العوامل، والجدران النارية والنسخ الاحتياطي الدوري يساهم في رفع مستوى أمن المعلومات وتقليل احتمالية التعرض للاختراقات وهو ما يتوافق مع ما توصلت إليه الدراسات الحديثة في مجال الأمن السيبراني

وبوجه عام يمكن القول إن نتائج الدراسة الحالية جاءت متوافقة بدرجة كبيرة مع معظم الدراسات السابقة مما يعزز موثوقية النتائج ويؤكد أهمية الاستثمار في الأمن السيبراني كأحد الركائز الأساسية لحماية المعلومات واستمرارية الأعمال

سادساً: خاتمة الفصل

تناول هذا الفصل عرض نتائج التحليل الإحصائي الخاصة بالدراسة بدءًا بوصف أفراد العينة، ثم اختبار صدق وثبات أداة الدراسة وتحليل استجابات المشاركين واختبار فرضيات البحث وربط النتائج بالدراسات السابقة.

وأظهرت النتائج أن أفراد العينة لديهم مستوى مرتفع من الوعي بالأمن السيبراني كما تبين أن المؤسسات تطبق عددًا من الممارسات الأمنية التي تسهم في حماية المعلومات والحد من المخاطر الإلكترونية كذلك أثبتت نتائج الدراسة وجود علاقة إيجابية بين تطبيق ممارسات الأمن السيبراني ومستوى حماية المعلومات الرقمية داخل المؤسسات

وبناءً على ذلك يمكن التأكيد على أن الأمن السيبراني أصبح عنصرًا أساسيًا في نجاح المؤسسات واستمرار أعمالها وأن تعزيز الوعي الأمني وتطوير السياسات الأمنية والاستثمار في التقنيات الحديثة، تمثل جميعها عوامل رئيسية في بناء بيئة رقمية آمنة

Cisco. (2024). What Is Cybersecurity? Cisco. <https://www.cisco.com/>

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems. ISO.

National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.

Stallings, W. (2021). Network Security Essentials: Applications and Standards (7th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

Aljohani, M., & Alqahtani, S. (2023). Cybersecurity awareness and information protection in organizations. *International Journal of Information Security Studies*, 15(2), 55–70.

Alshamrani, A. (2024). The impact of cybersecurity practices on organizational performance. *Journal of Information Systems Research*, 18(1), 101–118.

Saudi National Cybersecurity Authority. (2023). Essential Cybersecurity Controls (ECC-2:2023).