

عنوان المقرر: منهجية البحث في علوم الحاسوب

رمز المقرر: AI800

الوزن: ٢٠٪

المحاضر: د. محمد عنبر

تاريخ تسليم المواد: 20 يونيو 2026

تاريخ التسليم: 4 يوليو 2026

طريقة التسليم: إلكترونيًا عبر منصة التعلم الإلكتروني.

تقرير المهمة: مراجعة الأدبيات الهندسة الاجتماعية ودور العنصر البشري في الأمن السيبراني

رقم الطالب: 251000107

اسم الطالب: أنس حسن علي

جدول المحتويات:

- ملخص البحث
- التحليل النقدي
- الروابط
- التناقضات بين النتائج
- مصفوفة توليف مراجعة الأدبيات
- المراجع

ملخص البحث:

الورقة البحثية الأولى: الوقاية من هجمات الهندسة الاجتماعية

تدور مشكلة البحث في عدم تواجد مراجعة منهجية شاملة وفعالة تستند على جمع وتحليل الأساليب الهياكل والنماذج الوقائية من هجمات الهندسة الاجتماعية، بالإضافة إلى أن الدراسات السابقة تناولت حلول متفرقة ضيقة لم تصل إلى حدود التحليل الشامل.

تهدف هذه الدراسة إلى مراجعة نقدية ودقيقة للأدبيات السابقة والتي تتمحور حول أساليب ونماذج وأطر منع هجمات الهندسة الاجتماعية.

وتكمن أهمية هذه الدراسة في كون أنه لا توجد أبحاث سابقة محددة حول منع مثل هذه الهجمات، وتحللها بشكل فعال بصورة منهجية، مما يجعلها تسد فجوة بحثية في هذا المجال.

وقد اعتمد الباحثون على منهج المراجعة المنهجية للأدبيات، وفق منهجية Bryman & Bell، والتي بدورها مرت بثلاث مراحل رئيسة: التخطيط، والتنفيذ، وإعداد التقرير ونشر النتائج. ولجمع الدراسات، استخدم الباحثون كلمات البحث المتعلقة بالوقاية من هجمات الهندسة الاجتماعية، وركزوا البحث في أربع قواعد بيانات علمية هي Springer و Elsevier و IEEE و Wiley. نتج عن عملية البحث عن 86 دراسة، وبعد تطبيق ضوابط الاختيار من خلال مراجعة العناوين والملخصات واستبعاد ما هو بعيد عن الدراسات غير ذات الصلة، اعتمد الباحثون عن 53 دراسة في المراجعة النهائية.

وقد أظهرت الدراسة أن الوقاية من هجمات الهندسة الاجتماعية تعتمد بصورة رئيسة على ثلاثة أركان، هي: حملات التوعية الأمنية، وتحليل نقاط ضعف الضحايا، واستخدام بروتوكولات لتنظيم تبادل المعلومات عبر وسائل التواصل الاجتماعي. وبينما المراجعة أن من أكثر وسائل الوقاية فعالية، هي: حملات التوعية، بيد أن نجاحها مرتكز على نوعية الفئة المستهدفة، بالإضافة إلى ما هية محتوى الرسائل التوعية. وأوضحت الدراسة أن النماذج ذات الصلة في تقييم قابلية المستخدمين للهجمات تساعد في قياس مستوى المخاطر، بالإضافة إلى التنبؤ بالأفراد الأكثر عرضة للهندسة الاجتماعية. وتوصل الباحثون إلى أن السبب الرئيس المساهم في تعزيز حماية

المعلومات المتبادلة عبر الشبكات الاجتماعية من خلال إدارة تبادل المعلومات والاعتماد على نظام سمعة المستخدمين هو بروتوكول (Co-utile). وأوصت الدراسة ببتضمين أكثر من أسلوب وقائي، مثل البروتوكولات والأطر والنماذج وأساليب التقييم، للحصول على حماية أكثر فاعلية ضد هجمات الهندسة الاجتماعية.

وقد تم استخلاص قيتين من الدراسة، وهي:

لم تعتمد الدراسة على إجراء التجارب العلمية أو التطبيقات الميدانية للتحقق من فاعلية الحلول المقترحة، بل اعتمدت على التركيز على مراجعة الأدبيات السابقة.

تم حصر الدراسة على تحليل الدراسات المنشورة خلال الفترة (2018-2021)، وهذه بدوره يشير إلى عدم تضمين الدراسات الحديثة ذات الصلة المنشورة خارج هذه الفترة. (Syafitri, W., وآخرون)

الورقة البحثية الثانية: العوامل البشرية في هجمات التصيد الاحتيالي

وتدور مشكلة البحث في تزايد هجمات التصيد الاحتيالي، وأن محور اعتمادها يعود إلى استغلال العامل البشري، بالإضافة إلى أن الجوانب البشرية لا تحظى بالاهتمام الكافي لمجابهة مثل هذه الهجمات مقارنة بالجوانب التقنية.

تهدف هذه الدراسة إلى مراجعة منهجية للأدبيات التي تتصل بالعوامل البشرية في هجمات التصيد الاحتيالي وتحليلها.

وتتمثل أهمية هذه الدراسة في الإحصائيات التي تؤكد أن 95% من الحوادث الأمنية تعود إلى أخطاء بشرية، بالإضافة إلى الزيادات المتسارعة في مواقع التصيد الاحتيالي، مع ما صاحبه من خسائر عالمية للجرائم الالكترونية.

وقد اعتمد الباحثون على منهج المراجعة المنهجية للأدبيات وفقا لمنهجية كيتشنهام ، وذلك لدراسة العوامل البشرية في هجمات التصيد الاحتيالي. وارتكزت الدراسة على تحليل (52) منشورا علميا رئيسا نشر خلال الفترة من عام 2001م إلى مايو 2019م، حيث جرى تحليل هذه الدراسات وفق ثلاثة جوانب رئيسة ارتبط كل منها بأسئلة البحث، والتي بدورها مرت بثلاث مراحل أساسية، هي: البحث في المكتبات الرقمية، والبحث في المؤتمرات والمجلات العلمية، ثم البحث الرجعي ، مع تطبيق معايير للاختيار والاستبعاد حتى الوصول إلى الدراسات النهائية المعتمدة.

وقد أظهرت الدراسة أن هجمات التصيد الاحتيالي ترتبط ارتباطا وثيقا بالعوامل البشرية، وأن الأدبيات السابقة ركزت بصورة أكبر على الجوانب التقنية، بينما لا تزال المعرفة المنظمة بالعوامل البشرية في هذا المجال ضيقة. كما بينت الدراسة أن أكثر الموضوعات تناولا في الأدبيات تتمثل في السياسات الأمنية، وقابلية المؤسسات للتعرض للهجمات، ووعي المستخدمين، واستخدام النماذج المختلفة، وآليات الدفاع ضد هجمات التصيد الاحتيالي. وأوضحت الدراسة أن من أكثر وسائل التقليل من نجاح هذه الهجمات فعالية: التصميم الجيد لواجهات المستخدم، وتدريب المستخدمين، وتنظيم العوامل البشرية ضمن نطاقات عمل متخصصة. كما توصل الباحثون إلى أن أكثر العوامل البشرية استغلالا من قبل المهاجمين هي: نقص المعرفة، ونقص الموارد، وضعف الوعي، والأعراف الاجتماعية، والرضا الزائد. وأوصت الدراسة بضرورة تطوير مسار موحد لتنظيم العوامل البشرية في الأمن السيبراني، والاهتمام بتدريب المستخدمين، وتصميم أنظمة قوية أكثر قدرة على مقاومة هجمات التصيد الاحتيالي.

وقد تم استخلاص قيتين من الدراسة، وهي:

لم تتوصل الدراسات السابقة إلى إطار متفق عليه يحدد ويصنف العوامل البشرية في مجال الأمن السيبراني، مما جعل تحديد هذه العوامل وتفسيرها يتطلب جهدا كبيرا بسبب اختلاف المصطلحات المستخدمة بين الدراسات .

على الرغم من كثرة الحلول المقترحة، إلا أن هجمات التصيد الاحتيالي ما تزال فعالة ومتطورة باستمرار، الأمر الذي يتطلب تطوير حلول استباقية وبرامج تدريب فعالة تتناسب مع اختلاف فئات المستخدمين والتقنيات الحديثة. (Desolda, G., وآخرون)

الورقة البحثية الثالثة: الهندسة الاجتماعية عبر الإنترنت

وتدور مشكلة البحث في أن هجمات الهندسة الاجتماعية عبر الإنترنت ما تزال تحقق نجاحا كبيرا رغم كثرة الدراسات والحلول المقترحة، ويرى الباحثون أن السبب يكمن في وجود فجوة ومحدودية أثر بين الأساليب النفسية التي يستغلها المهاجمون وبين الأساليب التي تعتمد عليها الحلول الدفاعية الحالية.

تهدف هذه الدراسة إلى تحليل هجمات الهندسة الاجتماعية عبر الإنترنت ووسائل الدفاع ضدها من منظور العوامل النفسية والتقنيات النفسية، والكشف عن أسباب محدودة فعالية وسائل الدفاع الحالية، مع اقتراح مسار تنفيذي بحثي للدراسات المستقبلية.

وتكمن أهمية هذه الدراسة في أن هجمات الهندسة الاجتماعية ما تزال من أكثر التهديدات الإلكترونية انتشاراً وتأثيراً، على الرغم من كثرة الأبحاث ووسائل الحماية، كما توضح الدراسة وجود فجوة واضحة بين الأساليب النفسية التي يستغلها المهاجمون والأساليب التي تعتمد عليها وسائل الدفاع، مما يسهم في تفسير استمرار نجاح هذه الهجمات.

وقد اعتمد الباحثون على منهج المراجعة المسحية من منظور نفسي، حيث بدأوا بتحديد المنظور النفسي للدراسة، ثم جمع الأدبيات ذات الصلة، وبعد ذلك تنظيمها في أربعة محاور رئيسة هي: المفاهيم، والاستراتيجيات، والهجمات، ووسائل الدفاع، ثم تحليل العلاقات بينها لبيان الوضع الراهن، وأخيراً وضع تصور يتمثل في مسار تنفيذي للبحوث المستقبلية.

وقد أظهرت الدراسة أن هجمات الهندسة الاجتماعية عبر الإنترنت تستغل عدداً كبيراً من العوامل النفسية والتقنيات النفسية، في حين أن وسائل الدفاع الحالية لا تستفيد إلا من جزء محدود منها، وهو ما يفسر محدودية فاعلية الحلول الأمنية الحالية. كما توصل الباحثون إلى بناء تصور شامل يربط بين العوامل النفسية، والتقنيات النفسية، وأنواع الهجمات، ووسائل الدفاع، بما يسهم في توضيح الوضع الراهن لهذا المجال. وقدمت الدراسة مسار تنفيذي للبحوث المستقبلية تهدف إلى تطوير إطار شامل للأمن السيبراني النفسي، يساعد على فهم هجمات الهندسة الاجتماعية بصورة أعمق وتصميم وسائل دفاع أكثر كفاءة. وأكدت الدراسة أهمية تطوير برامج تدريبية متقدمة، وتحسين وسائل الدفاع الآلية، والاستفادة من العوامل والتقنيات النفسية في بناء حلول أمنية قادرة على مواجهة الهجمات المستقبلية.

وقد تم استخلاص قيتين من الدراسة، وهي:

لم تقدم الدراسة إطاراً عملياً أو تطبيقاً تجريبياً للتحقق من فاعلية المسار التنفيذي المقترح، وإنما اكتفت بتقديم تصور نظري قائم على مراجعة وتحليل الدراسات السابقة.

أشارت الدراسة إلى وجود العديد من المشكلات البحثية المفتوحة المتعلقة بتطوير وسائل الدفاع والتدريب واكتشاف الهجمات، مما يدل على أن الحلول الحالية لا تزال غير مكتملة وتحتاج إلى مزيد من الدراسات والتطوير. (Longtchi, T. T., وآخرون)

الورقة البحثية الرابعة: تحليل الوعي بالهندسة الاجتماعية بين الطلاب والمحاضرين
وتدور مشكلة البحث في تزايد هجمات الهندسة الاجتماعية نتيجة الانتشار الواسع لاستخدام التقنيات الرقمية والإنترنت، مع وجود ضعف في وعي المستخدمين بالأمن السيبراني، مما يعرض البيانات الحساسة، وخاصة في المؤسسات الأكاديمية، لخطر الاختراق وسرقة المعلومات.

تهدف هذه الدراسة إلى تقييم مستوى معرفة الطلبة وأعضاء هيئة التدريس بالأمن السيبراني، وتحليل مستوى وعيهم بهجمات الهندسة الاجتماعية واختراقات البيانات، والكشف عن العوامل التي تؤثر في هذا الوعي.

وتكمن أهمية هذه الدراسة في أنها تسلط الضوء على مستوى الوعي بهجمات الهندسة الاجتماعية داخل البيئة الجامعية، كما أنها تتميز بدراسة كل من الطلبة وأعضاء هيئة التدريس معاً، على خلاف معظم الدراسات السابقة التي ركزت على الطلبة فقط، مما يسهم في تقديم صورة أشمل عن واقع الوعي بالأمن السيبراني، ويساعد في تطوير برامج التدريب وتعزيز أنظمة الحماية.

وقد اعتمد الباحثون على المنهج الكمي، من خلال إعداد استبانة إلكترونية باستخدام Google Forms، وزعت على طلبة الدراسات الأولية والعليا وأعضاء هيئة التدريس في جامعة السليمانية. بلغ عدد المشاركين 1779 مشاركاً، منهم 1554 طالباً و225 من أعضاء هيئة التدريس. وتكونت الاستبانة من (24) سؤالاً موزعة على قسمين: الأول للبيانات الديموغرافية، والثاني لقياس الوعي بهجمات الهندسة الاجتماعية، والتي شملت ستة محاور رئيسية هي: التصيد الاحتيالي، والرسائل النصية الاحتيالية، والطعم، والذرائع باستخدام الذكاء الاصطناعي والمقايضة والتسلل

المرافق. واستخدم الباحثون مقياس ليكرت في عدد من الأسئلة، كما تم تحليل البيانات باستخدام برنامج IBM SPSS الإصدار (22)، والتحقق من ثبات أداة الدراسة باستخدام معامل كرونباخ ألفا، والذي بلغ (0.74).

وقد أظهرت الدراسة أن مستوى الوعي بهجمات الهندسة الاجتماعية لدى الطلبة وأعضاء هيئة التدريس تأثر بعدة عوامل، أبرزها نقص الخبرة، والأخطاء البشرية، وضعف التدريب في مجال الأمن السيبراني. كما بينت النتائج وجود ضعف في معرفة المشاركين بوسائل الحماية، مثل الجدار الناري وبرامج مكافحة الفيروسات، بالإضافة إلى استخدام كلمات مرور متشابهة لحسابات متعددة، مما يزيد من احتمالية التعرض للاختراق. وأوضحت الدراسة أن أكثر أساليب الهندسة الاجتماعية تأثيراً على المشاركين كانت التصيد الاحتيالي، والرسائل النصية الاحتيالية، والطعم، والذرائع باستخدام الذكاء الاصطناعي، في حين تبين أن التصيد الاحتيالي الموجه يعد أكثر الأساليب خطورة. كما أوصت الدراسة بتعزيز الوعي من خلال تقديم دورات وورش عمل متخصصة، وتوفير أدوات الحماية، وتطوير المناهج المتعلقة بالأمن السيبراني داخل المؤسسات الأكاديمية.

وقد تم استخلاص قيتين من الدراسة، وهي:

اقتصرت الدراسة على جامعة السليمانية، ولم تشمل جامعات أخرى، وذلك بسبب محدودية الوقت، مما يحد من إمكانية تعميم النتائج.

لم يكن عدد المشاركين من الطلبة وأعضاء هيئة التدريس متساوياً، نظراً لأن عدد الطلبة في الجامعة أكبر بكثير من عدد أعضاء هيئة التدريس، مما قد يؤثر في توازن نتائج الدراسة. (Abdulla, R. وآخرون)

الورقة البحثية الخامسة: استخلاص العوامل الرئيسية لسلوكيات النظافة الإلكترونية بين مهندسي البرمجيات

وتدور مشكلة البحث في عدم وضوح العوامل المؤثرة في سلوك النظافة السيبرانية لدى مهندسي البرمجيات، واستمرار ضعف ممارسات الأمن السيبراني رغم وجود برامج التوعية والتدريب، مما يؤدي إلى زيادة التعرض للهجمات السيبرانية داخل مؤسسات تطوير البرمجيات.

تهدف هذه الدراسة إلى إجراء مراجعة منهجية للأدبيات العلمية لاستخلاص العوامل الرئيسية المؤثرة في سلوك النظافة السيبرانية لدى مهندسي البرمجيات، وتصنيفها إلى عوامل إيجابية وسلبية، وبيان أثرها في تعزيز ممارسات الأمن السيبراني.

وتكمن أهمية هذه الدراسة في أنها تساهم في سد الفجوة البحثية المتعلقة بفهم العوامل المؤثرة في سلوك النظافة السيبرانية لدى مهندسي البرمجيات، كما تقدم مرجعا علميا يساعد الباحثين والمؤسسات وصناع القرار على تعزيز ممارسات الأمن السيبراني والحد من التهديدات الإلكترونية.

وقد اعتمد الباحثون على منهج المراجعة المنهجية للأدبيات وفقا لمنهجية كيتشنهام، والتي مرت بثلاث مراحل رئيسية هي: التخطيط، وإجراء المراجعة، وتوثيق النتائج. ولجمع الدراسات استخدم الباحثون استراتيجيات بحث محددة تضمنت كلمات مفتاحية مرتبطة بالنظافة السيبرانية وسلوك الأمن السيبراني، واعتمدوا على أربع قواعد بيانات علمية هي: IEEE Xplore، وScienceDirect، وSpringerLink، وEmerald Insight. وأسفرت عملية البحث عن 5270 دراسة، وبعد تطبيق معايير الاشتغال والاستبعاد وإزالة الدراسات المكررة وتقييم الجودة، اعتمد الباحثون 35 دراسة فقط في المراجعة النهائية.

وقد أظهرت الدراسة أن سلوك النظافة السيبرانية لدى مهندسي البرمجيات يتأثر بمجموعة من العوامل الشخصية والاجتماعية والإدارية والبيئية والتقنية، حيث تمكن الباحثون من استخلاص 19 عاملا مؤثرا، وتصنيفها إلى عوامل ذات تأثير إيجابي وأخرى ذات تأثير سلبي في سلوك النظافة السيبرانية. وبينت الدراسة أن فهم العلاقة بين هذه العوامل يساعد المؤسسات على تطوير ممارسات أمنية أكثر فاعلية، وتعزيز ثقافة الأمن السيبراني لدى مهندسي البرمجيات. كما أوضحت أن تطبيق ممارسات النظافة السيبرانية بصورة منهجية يساهم في رفع مستوى الحماية وتقليل المخاطر والتهديدات السيبرانية، ويساعد مهندسي البرمجيات على تطوير وصيانة أنظمة أكثر أمنا.

وقد تم استخلاص قيديين من الدراسة، وهما:

اقتصرت الدراسة على مراجعة الأدبيات المنشورة خلال الفترة (2010-2020)، مما يعني عدم تضمين الدراسات المنشورة بعد هذه الفترة.

اقتصرت الدراسة على تحليل الدراسات المتعلقة بمهندسي البرمجيات، لذلك قد لا يمكن تعميم نتائجها على جميع فئات المستخدمين أو القطاعات الأخرى. (Kalhoro, S., وآخرون)

الورقة البحثية السادسة: تصنيف الهجمات ودراسة آليات الدفاع ضد هجمات الهندسة الاجتماعية الدلالية

وتدور مشكلة البحث في عدم وجود تصنيف شامل ومنهجي لهجمات الهندسة الاجتماعية الدلالية وآليات الدفاع عنها، إذ إن معظم وسائل الحماية الحالية تركز على أنواع محددة من الهجمات، وتفتقر إلى القدرة على مواجهة الأساليب المتغيرة والمتطورة للمهاجمين بصورة شاملة.

تهدف هذه الدراسة إلى بناء تصنيف شامل لهجمات الهندسة الاجتماعية الدلالية، واستعراض وتحليل آليات الدفاع المقترحة ضدها، وبيان مدى فاعليتها ونطاق تطبيقها، بما يساعد على تطوير وسائل حماية أكثر شمولية ومرونة.

وتكمن أهمية هذه الدراسة في أنها تقدم تصنيفاً منهجياً لهجمات الهندسة الاجتماعية الدلالية وآليات الدفاع المرتبطة بها، مما يساعد الباحثين والمختصين على فهم العلاقات بين أنواع الهجمات المختلفة، وتطوير حلول دفاعية قادرة على مواجهة الهجمات الحالية والمستقبلية بصورة أكثر فاعلية.

اعتمد الباحثان على مراجعة شاملة للأدبيات العلمية المتعلقة بهجمات الهندسة الاجتماعية، ثم قاما بتحليل الهجمات وآليات الدفاع المنشورة في الدراسات السابقة، وبعد ذلك طوّرا تصنيفاً منهجياً (Taxonomy) ينظم الهجمات وفق خصائصها المشتركة بدلا من الاكتفاء بتصنيفها حسب نوع الهجوم. كما استخدموا هذا التصنيف لتحليل وسائل الدفاع وتحديد مدى قدرتها على مواجهة أنواع الهجمات المختلفة.

وقد أظهرت الدراسة أن وسائل الدفاع التقنية التقليدية لا تزال تواجه صعوبة في التصدي لمختلف أنواع هجمات الهندسة الاجتماعية، ولا سيما الهجمات الحديثة والمتطورة. وللتغلب على ذلك، قدم الباحثان تصنيفاً علمياً (Taxonomy) يعتمد على تحليل مكونات الهجوم وخصائصه بدلا من تصنيفه وفق نوعه فقط، مما يساهم في فهم أعمق لآليات الهجوم وتحديد وسائل الدفاع المناسبة لها. كما بينت الدراسة أن ربط وسائل الدفاع بخصائص الهجمات المشتركة، بدلا من التركيز على هجوم محدد،

يساعد في تطوير آليات دفاع أكثر شمولاً ومرونة، ويعزز قدرة الأنظمة الأمنية على مواجهة الهجمات الحالية والمستقبلية، مع التأكيد على أهمية دمج الحلول التقنية مع برامج التوعية والتدريب الأمني لتحقيق حماية أكثر فاعلية.

وقد تم استخلاص قيتين من الدراسة، وهما:

اقتصرت الدراسة على مراجعة وتحليل هجمات الهندسة الاجتماعية ووسائل الدفاع اعتماداً على الأدبيات العلمية، دون إجراء تجارب عملية أو تطبيقات ميدانية للتحقق من فاعلية التصنيف المقترح.

ركزت الدراسة على تطوير تصنيف نظري لهجمات الهندسة الاجتماعية ووسائل الدفاع المرتبطة بها، لذلك قد يتطلب تطبيق هذا التصنيف وتقييم فعاليته في البيئات الواقعية إجراء دراسات وتجارب مستقبلية. (Heartfield, R., & Loukas, G.)

تحليل نقدي:

قدمت الورقة البحثية الأولى مرجعاً نظرياً قوياً متصلاً بالبعد النفسي للهندسة الاجتماعية، وفي نفس الوقت تحتاج النتائج إلى تدعيمها بشيء من الدراسات التطبيقية الميدانية لتأكيد فاعليتها. وأثبتت الورقة البحثية الثانية أسباب نجاح هجمات التصيد، ومع ذلك لم تقدم إطاراً عملياً للحماية. ووصفت الورقة البحثية الثالثة الهجمات الإلكترونية وصفاً جيداً، وفي المقابل تركت مشكلات بحثية تحتاج إلى مزيد من الدراسات والتطوير. وبرهنت الورقة البحثية الرابعة أدلة ميدانية واسعة حول مستوى الوعي الأمني، وفي المقابل اقتصرت على جامعة واحدة وفي دولة واحدة. وتعد الورقة البحثية الخامسة مرجعية مهمة لاستيعاب سلوكيات النظافة السيبرانية، إلا أنها اقتصرت على الدراسات المنشورة حتى عام 2020 وركزت على بيئة مهندسي البرمجة. وأسست الورقة البحثية السادسة أساساً علمياً رصيناً لتصنيف الهجمات، إلا أنها غلبت عليها الجانب النظري على الجانب التطبيقي.

الروابط

التناقضات بين النتائج:

اتفقت الدراسات على أهمية التوعية الأمنية، واختلفت في تفسير أسباب نجاح وهيمنة هجمات الهندسة الاجتماعية. فبينما ركزت دراسة Longtchi وآخرين (2024) على العوامل النفسية باعتبارها السبب الرئيس، ركزت دراسة Abdulla وآخرين (2023) على نقص المعرفة والتدريب، في حين أوضحت دراسة Kalhoro وآخرين (2021) أن سلوك النظافة السيبرانية يتأثر بعوامل شخصية واجتماعية وتقنية متعددة. أما دراسة Loukas و Heartfield (2015) فقد ركزت على تصنيف الهجمات ووسائل الدفاع دون التعمق في العوامل البشرية.

مصفوفة توليف مراجعة الأدبيات:

الدراسة	الهدف	المنهجية	أبرز النتائج	القيود
الدراسة الأولى	تحليل هجمات الهندسة الاجتماعية من منظور نفسي وربط العوامل النفسية بأساليب الإقناع والهجمات والدفاعات.	مراجعة منهجية للأدبيات (Systematization of Knowledge - SoK).	حددت العوامل النفسية وتقنيات الإقناع المستغلة في الهجمات، وقدمت خارطة طريق لتطوير دفاعات أكثر فاعلية.	اقتصرت على الأدبيات المتاحة ولم تختبر النموذج تجريبياً.
الدراسة الثانية	قياس مستوى الوعي بالهندسة الاجتماعية لدى طلبة وأعضاء هيئة التدريس في جامعة السليمانية.	دراسة كمية باستخدام استبانة إلكترونية شملت (1779) مشاركاً.	أظهرت انخفاض مستوى المعرفة ببعض أساليب الهندسة الاجتماعية، والحاجة إلى التدريب والتوعية المستمرة.	اقتصرت على جامعة واحدة، مع عدم توازن أعداد الطلبة وأعضاء هيئة التدريس.
الدراسة الثالثة	استخراج العوامل المؤثرة في سلوك النفاذة السيبرانية لدى مهندسي البرمجيات.	مراجعة منهجية للأدبيات (SLR) شملت (35) دراسة منشورة بين 2010-2020.	حددت (19) عاملاً مؤثراً في سلوك النفاذة السيبرانية، وصنفتها إلى عوامل إيجابية وسلبية.	اقتصرت على الدراسات المنشورة خلال 2010-2020 وعلى مهندسي البرمجيات فقط.
الدراسة الرابعة	تصنيف هجمات الهندسة الاجتماعية (Semantic Attacks) واليات الدفاع ضدها.	دراسة تصنيفية (Taxonomy) مدعومة بمراجعة شاملة لآليات الدفاع.	قدمت تصنيفاً موحداً للهجمات وفق مكوناتها، وربطت كل فئة بوسائل الدفاع المناسبة، ودعت إلى دمج الحلول التقنية مع التوعية البشرية.	لم يتم التحقق من التصنيف عملياً من خلال تطبيق أو تجربة ميدانية.
الدراسة الخامسة	تحليل تأثير العوامل البشرية في نجاح هجمات الهندسة الاجتماعية وقياس مستوى الوعي الأمني لدى المستخدمين.	دراسة تجريبية باستخدام استبيانات وتحليل إحصائي لسلوك المستخدمين.	أظهرت أن نقص الوعي الأمني والثقة الزائدة وضعف التدريب من أكثر العوامل التي تزيد من قابلية المستخدمين للتعرض للهجمات، وأوصت ببرامج توعية مستمرة.	اقتصرت الدراسة على عينة محددة من المستخدمين، مما قد يحد من إمكانية تعميم النتائج على جميع البيئات.
الدراسة السادسة	مراجعة أساليب الهندسة الاجتماعية وآليات الحماية وتقييم الحلول الأمنية المقترحة.	مراجعة أدبيات وتحليل مقارنة للدراسات السابقة.	بينت أن الحلول التقنية وحدها غير كافية، وأن الجمع بين الإجراءات التقنية والتوعية والتدريب والسياسات الأمنية يوفر حماية أكثر فاعلية ضد الهجمات.	اعتمدت على تحليل الدراسات السابقة دون إجراء تجارب عملية أو تقييم ميداني للحلول المقترحة.

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). *Social Engineering Attacks Prevention: A Systematic Literature Review*. *IEEE Access*, 10, 39325–39343. <https://doi.org/10.1109/ACCESS.2022.3162594>

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). *Human Factors in Phishing Attacks: A Systematic Literature Review*. *ACM Computing Surveys*, 54(8), Article 173, 1-35. <https://doi.org/10.1145/3469886>

Longtchi, T. T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2024). *Internet-based social engineering: Psychology, attacks, and defenses: A survey*. **Proceedings of the IEEE**, 112(3), 210–252. <https://doi.org/10.1109/JPROC.2024.3379855>

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., et al. (2023). *Analysis of Social Engineering Awareness Among Students and Lecturers*. *IEEE Access*, 11, 101098–101108. <https://doi.org/10.1109/ACCESS.2023.3318385>

Kalhor, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). *Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review*. **IEEE Access**, 9, 99339–99359. <https://doi.org/10.1109/ACCESS.2021.3097490>

Heartfield, R., & Loukas, G. (2015). *A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks*. *ACM Computing Surveys*, 48(3), Article 37. <https://doi.org/10.1145/2835375>