

العوامل البشرية في هجمات التصيد الاحتيالي
(دراسة منهجية)

Contents

ملخص	3
مقدمة	4
الخلفية	4
بيان المشكلة	5
الاهداف البحثية	5
نطاق البحث	6
مراجعة الادبيات	6
منهجية البحث	7
المرحلة الأولى: التركيز على الكشف والتصفيه التقنية	7
المرحلة الثانية: التوسع في تصنيف وفهم هجمات التصيد	7
المرحلة الثالثة: الاهتمام بالعامل البشري في الأمن السيبراني	8
المرحلة الرابعة: الربط بين العامل البشري والتصيد الاحتيالي	8
الاعتبارات الاخلاقية	8
القيود	8
النتائج المتوقعة	9
رسم الجدول الزمني	10
المراجع	11

ملخص

تزايدت هجمات التصيد الاحتيالي مع التطور المستمر والمتسارع في التقنيات الرقمية، وأصبح العامل البشري أحد العناصر الرئيسة والمؤثرة التي تستغلها هذه الهجمات للوصول إلى المستخدمين والأنظمة. وعلى الرغم من التطور المستمر في الحلول التقنية لمواجهة التصيد الاحتيالي، لا يزال الجانب البشري بحاجة إلى مزيد من الدراسة والبحث، ولا سيما فيما يتعلق بسلوك المستخدم ووعيه وقدرته على التمييز بين المحاولات الاحتيالية من غيرها من المحاولات الأخرى. يهدف هذا البحث إلى دراسة العوامل البشرية المرتبطة بهجمات التصيد الاحتيالي، وتحديد أبرز العوامل التي تسهم في نجاح هذه الهجمات، والكشف عن الفجوات البحثية في الأدبيات السابقة. ولتحقيق ذلك، اعتمدت الدراسة منهجية المراجعة المنهجية للأدبيات (SLR) لتحليل الدراسات ذات الصلة وفق معايير محددة للبحث والاختيار والاستخراج والتحليل. وأظهرت نتائج المراجعة أهمية عدد من العوامل البشرية، من بينها الوعي الأمني، والمعرفة، والسلوك، والعوامل النفسية والمعرفية، في التأثير في استجابة المستخدم لمحاولات التصيد. كما كشفت المراجعة عن الحاجة إلى تعزيز التكامل بين الحلول التقنية والتوعية والتدخلات التي تستهدف العامل البشري. وتوفر هذه الدراسة أساساً لفهم الدور الذي يؤديه العامل البشري في هجمات التصيد الاحتيالي، وتحديد الاتجاهات التي يمكن أن تسهم في تطوير وسائل أكثر فاعلية للحد من هذه التهديدات.

مقدمة

مع التقدم المتسارع في التكنولوجيا، ومع كثرة الاعتماد اليومي له، والتفاعل معه بعدة طرق في كل مجالات الحياة، وما أضافه على حياتنا من اضافات ايجابية ذات قيمة عالية، ومع ذلك كله برزت احداث حساسة أثرت بصورة كبيرة على بعض هذه الايجابيات وجعلتها أرض خصبة لتنفيذ بعض المخططات او الاجندات الخادعة والاستغلال المبني على نقص المعرفة عند بعض البشر (1، 2، 3، 4، 5).

ومع تطور وتسارع هذه الاحداث الخبيثة، قابلتها تطورات مجابهة لها للحد من منعها أو التقليل منها بقدر المستطاع، بل دعت إلى ايجاد حلول استباقية قبل وقوع أي تهديدات مستقبلية ذات تأثير كبير معتمدة في ذلك على الانسان، ومحدودية أداء مهامه في الوقت الواحد، والذي يعد اساس المشكلة إما بالمساهمة المباشرة في تعزيزها، أو السماح بتمريرها، بسبب نقص المعرفة، وقلة البرامج الداعمة لتوضيح ذلك للأفراد بالاضافة إلى إهمال البرامج التقنية التي قد تحد أو تقلل من هذه التهديدات (6).

ويسعى هذا البحث لمعالجة هذا الفجوات من خلال طرح اطار شامل على هجمات التصيد الاحتيالي وعلاقتها بالعوامل البشرية، والحيلولة دون وقوعها.

الخلفية

تسارعت التقنية وتطورت في فترة زمنية وجيزة، وتوازي معها وتسابق تقنيات خبيثة أصبحت حبر عثره في طريق تقدمها، وهذا بدوره يدعو إلى تحجيم أثر هذه التهديدات

¹ Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8), 1–35. DOI: 10.1145/3469886

² A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani. 2013. A survey of phishing email filtering techniques. IEEE Communications Surveys Tutorials 15, 4 (2013), 2070–2090. <https://doi.org/10.1109/SURV.2013.030713.00020>

³ Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. 2018. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications 106 (2018), 1–20. <https://doi.org/10.1016/j.eswa.2018.03.050>

⁴ M. Khonji, Y. Iraqi, and A. Jones. 2013. Phishing detection: A literature survey. IEEE Communications Surveys Tutorials 15, 4 (2013), 2091–2121. <https://doi.org/10.1109/SURV.2013.032213.00009>

⁵ Xichen Zhang and Ali A. Ghorbani. 2020. Human factors in cybersecurity: Issues and challenges in big data. In Security, Privacy, and Forensics Issues in Big Data. IGI Global, 66–96. <https://doi.org/10.4018/978-1-5225-9742-1.ch003>

⁶ Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8), 1–35. DOI: 10.1145/3469886.

السيبرانية الخبيثة، والحيلولة دون وقوعها، وهذا أصبح واضحا جليا في هجمات التصيد الاحتيالي، وما رافقه من مساعدات بشرية تعود الى جهل الانسان بخطورة واهمية هذا الجانب، لذا وجه هذا البحث بوصلته للمساعدة في تضيق هذه الفجوة، وايجاد الحلول المناسبة لانهاء تهديدها.

بيان المشكلة

وتدور مشكلة البحث في تزايد هجمات التصيد الإحتيالي، وأن محور اعتمادها يعود إلى استغلال العامل البشري^(7،8،9)، بالإضافة إلى أن الجوانب البشرية لا تحظى بالاهتمام الكافي لمقاومة مثل هذه الهجمات مقارنة بالجوانب التقنية، ولا سيما ما يتعلق بوعي المستخدم وسلوكه المعرفي وقدرته على التمييز بين المحاولات الاحتيالية والاستجابة لها بكفاءة وفاعلية⁽¹⁰⁾.

الاهداف البحثية

مراجعة شاملة لمنهجية الأدبيات المتعلقة بالعوامل البشرية المؤثرة في هجمات التصيد الاحتيالي وتحليلها.

- تحديد القصور والتحديات والقيود الرئيسة التي واجهت هذه الدراسة، كما تم ذكره في الأدبيات في التكاليف الأول.
- التقييم النقدي للحلول الحالية.

⁷ A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani. 2013. A survey of phishing email filtering techniques. IEEE Communications Surveys Tutorials 15, 4 (2013), 2070–2090.

<https://doi.org/10.1109/SURV.2013.030713.00020>

⁸ Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. 2018. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications 106 (2018), 1–20.

<https://doi.org/10.1016/j.eswa.2018.03.050>

⁹ M.Khonji, Y.Iraqi, and A.Jones. 2013. Phishing detection: A literature survey. IEEE Communications Surveys Tutorials 15, 4 (2013), 2091–2121. <https://doi.org/10.1109/SURV.2013.032213.00009>

¹⁰ A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani. 2013. A survey of phishing email filtering techniques. IEEE Communications Surveys Tutorials 15, 4 (2013), 2070–2090.

<https://doi.org/10.1109/SURV.2013.030713.00020>

نطاق البحث

سلط الضوء هذا الحث على دراسة العوامل البشرية المرتبطة بهجمات التصيد الاحتيالي، وذلك من خلال مراجعة وتحليل الدراسات العلمية المنشورة في هذا المجال وفق منهجية المراجعة المنهجية للأدبيات (SLR). ويغطي نطاق البحث العوامل المقترنة بسلوك المستخدم، والوعي الأمني، والأخطاء البشرية، والعوامل النفسية والسلوكية التي قد تكون ذات تأثير مباشر في مدى استجابة الناس وتقبلهم لمحاولات التصيد الاحتيالي أو الوقوع في فخها.

ويتمحور البحث حول الدراسات التي تستعرض أبعاد العلاقة بين العامل البشري وهجمات التصيد الاحتيالي، ولا يستعرض الجوانب التقنية المطلقة للهجمات، مثل تحليل البرمجيات الخبيثة أو اختبار الاختراق، ما لم تكن هذه الجوانب ذات ارتباط وثيق بالعامل البشري محل الدراسة.

مراجعة الادبيات

تعقدت هجمات التصيد الإحتيالي في الآونة الأخيرة، وأثرت تأثير قوي على العديد من الاقتصادات العالمية، بما فيها الدول التي تعد مهتمة بصورة كبيرة بالتقنية، وعزا أصحاب الاهتمام هذا التصاعد الى العامل البشري والقدرة على استغلاله، بالإضافة إلى وجود قصور في الاهتمام بالجانب البشري للتصدي لهذه الهجمات مقارنة بالجوانب التقنية¹¹. قام المومني وآخرون¹² باستعراض شامل لأحدث الابحاث في هذا المجال، مناقشا بالتفاصيل والحلول أساليب الحماية من هجمات البريد الإلكتروني الاحتيالية. وأكد خنجي وآخرون¹³ في دراستهم الاستقصائية على عدم وجود حل واحد شامل للتخفيف من جميع الثغرات الأمنية، وأوجدوا حولا تقنية بصورة عامة لجميع فئات تقنيات التخفيف من التصيد الاحتيالي مثل: الكشف، والدفاع الهجومي، والتصحيح، والوقاية. وتطرقت بعض التغطيات لجزئية هجمات التصيد في بعض

¹¹ Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. 2018. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications 106 (2018), 1–20. <https://doi.org/10.1016/j.eswa.2018.03.050>

¹² A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani. 2013. A survey of phishing email filtering techniques. IEEE Communications Surveys Tutorials 15, 4 (2013), 2070–2090. <https://doi.org/10.1109/SURV.2013.030713.00020>

¹³ M. Khonji, Y. Iraqi, and A. Jones. 2013. Phishing detection: A literature survey. IEEE Communications Surveys Tutorials 15, 4 (2013), 2091–2121. <https://doi.org/10.1109/SURV.2013.032213.00009>

المراجعات الادبية في موضوع العوامل البشرية في الأمن السيبراني، كما في دراسة ديسولدا وآخرون(2022)¹⁴ ، والتي عمدت إلى تحليل الدراسات السابقة مع تدعيمها بأبرز العوامل المؤثرة التي يتعرض لها المستخدمون في مجال التصيد الإلكتروني، وتعزيزها ببعض التوجهات للبحوث في المستقبل. كما زاد تأكيد دراسة خادكا وأولاه (2025)¹⁵ على أن هجمات التصيد الإلكتروني تعد من أبرز ركائز التهديدات التي تستهدف استغلال السلوك البشري لتحقيق نزوات المخترقين.

منهجية البحث

اعتمدت هذه الدراسة على منهجية المراجعة المنهجية للأدبيات (SLR) بهدف تحديد وتحليل الدراسات السابقة التي تناولت العوامل البشرية المرتبطة بهجمات التصيد الاحتيالي. وتم اتباع منهجية منظمة لجمع الدراسات ذات الصلة، وفرزها وفق معايير محددة، ثم استخراج البيانات وتحليلها ومقارنتها بهدف تحديد الاتجاهات البحثية والفجوات القائمة في هذا المجال.

المرحلة الأولى: التركيز على الكشف والتصفية التقنية

ركزت الدراسات المبكرة بصورة أساسية على تطوير تقنيات قادرة على اكتشاف رسائل التصيد الاحتيالي وتصنيفها. فقد تناول المومني وآخرون (2013) تقنيات ترشيح رسائل البريد الإلكتروني الاحتيالية، بينما استعرض خنجي وآخرن (2013) الأدبيات المتعلقة بتقنيات اكتشاف التصيد. ويعكس ذلك تركيزا واضحا على مواجهة التصيد من منظور تقني.

المرحلة الثانية: التوسع في تصنيف وفهم هجمات التصيد

انتقل الاهتمام البحثي لاحقا إلى دراسة التصيد الاحتيالي بصورة أوسع، بما في ذلك أنواعه ونواقل الهجوم والأساليب التقنية المستخدمة في تنفيذه. ويظهر ذلك في دراسة تشيو وآخرون(2018) ، التي قدمت مسحا لأنواع هجمات التصيد ونواقلها والأساليب

¹⁴ Giuseppe Desolda, Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Computing Surveys*, 2022.

¹⁵ Khadka, K., & Ullah, A. B. (2025). Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal. *International Journal of Information Security*.

التقنية المرتبطة بها. وتمثل هذه المرحلة توسعا في فهم طبيعة الهجمات، بدل الاقتصار على آليات اكتشافها.

المرحلة الثالثة: الاهتمام بالعامل البشري في الأمن السيبراني

مع اتساع فهم طبيعة التهديدات السيبرانية، برز العامل البشري بوصفه أحد العناصر المهمة في منظومة الأمن السيبراني. وفي هذا السياق، قدم خداكا وابو بركات الله (2025)مراجعة للعوامل البشرية في الأمن السيبراني، مما يعكس توجهها بحثيا يتجاوز الجوانب التقنية إلى دراسة تأثير الإنسان وسلوكه في البيئة الأمنية.

المرحلة الرابعة: الربط بين العامل البشري والتصيد الاحتيالي

تتمثل المرحلة التي يركز عليها البحث الحالي في دراسة العلاقة المباشرة بين العوامل البشرية وهجمات التصيد الاحتيالي. ويشمل ذلك دراسة العوامل السلوكية والنفسية والمعرفية، ومستوى الوعي الأمني، وغيرها من العوامل التي قد تؤثر في قابلية المستخدم للاستجابة لمحاولات التصيد أو الوقوع ضحية لها. ومن خلال تحليل هذه الأدبيات يمكن تحديد أوجه الاتفاق والاختلاف بين الدراسات، والكشف عن الفجوات البحثية التي لا تزال بحاجة إلى مزيد من الدراسة.

الاعتبارات الاخلاقية

التزمت هذه الدراسة بمبادئ الأمانة العلمية والنزاهة البحثية أثناء جمع الدراسات وتحليلها وعرض نتائجها. وتمت المحافظة على توثيق المصادر ونسب المعلومات والأفكار إلى أصحابها وفق الأسلوب العلمي المعتمد، مع تجنب تحريف نتائج الدراسات أو عرضها بصورة قد تؤدي إلى استنتاجات غير دقيقة. ونظرا إلى أن الدراسة تعتمد على مصادر منشورة ولا تتضمن جمع بيانات مباشرة من المشاركين أو التعامل مع بيانات شخصية، فإنها لا تتطلب جمع بيانات بشرية مباشرة ضمن نطاقها الحالي.

القيود

تواجه هذه الدراسة عددا من القيود التي ينبغي أخذها في الاعتبار عند تفسير نتائجها. أولا، اقتصرت عملية البحث على قواعد البيانات العلمية المحددة ضمن استراتيجية البحث، مما قد يؤدي إلى عدم الوصول إلى بعض الدراسات ذات الصلة المنشورة في

مصادر أخرى. ثانياً، اقتصرَت الدراسة على الدراسات التي تستوفي معايير الإدراج والاستبعاد المحددة مسبقاً، مما قد يؤدي إلى استبعاد بعض الدراسات التي تتناول الموضوع من زوايا مختلفة.

كما قد يؤدي اختلاف المناهج والأدوات والعينات المستخدمة في الدراسات المشمولة إلى وجود تفاوت في نتائجها، مما قد يحد من إمكانية المقارنة المباشرة بينها. إضافة إلى ذلك، فإن الاعتماد على الدراسات المنشورة قد يجعل النتائج عرضة لتحيز النشر، حيث قد تكون الدراسات ذات النتائج الواضحة أكثر احتمالاً للنشر من غيرها.

وعليه، ينبغي تفسير نتائج هذه المراجعة في ضوء هذه القيود، مع اعتبارها أساساً يمكن البناء عليه في الدراسات المستقبلية.

النتائج المتوقعة

أظهرت نتائج المراجعة المنهجية أن العوامل البشرية تمثل جانباً متكرراً في الدراسات المتعلقة بهجمات التصيد الاحتيالي، مع تفاوت واضح في طبيعة العوامل التي ركزت عليها الدراسات. وأظهر تحليل الدراسات المشمولة أن الوعي الأمني ونقص المعرفة المتعلقة بأساليب التصيد من العوامل التي حظيت باهتمام ملحوظ، إلى جانب عدد من العوامل النفسية والسلوكية المرتبطة باتخاذ القرار والاستجابة لمحاولات التصيد.

كما أظهرت المقارنة بين الدراسات وجود اختلاف في المناهج والأدوات المستخدمة لدراسة سلوك المستخدم، مما أدى إلى تفاوت في النتائج المتعلقة بدرجة تأثير كل عامل. وأظهر التحليل كذلك وجود اهتمام متزايد بدراسة الجانب البشري إلى جانب الحلول التقنية المستخدمة في مواجهة التصيد الاحتيالي.

رسم الجدول الزمني

المرحلة	المهمة	المدة
1	مراجعة الأدبيات	عدة أيام
2	وضع أسئلة البحث	عدة أيام
3	تطوير منهجية	عدة أيام
4	جمع البيانات	عدة أيام
5	تحليل البيانات	عدة أيام
6	تطوير الإطار	عدة أيام
7	صياغة الرسالة	عدة أيام
8	تعديلات	عدة أيام
9	التسليم النهائي	عدة أيام
10	تحضير العرض	عدة أيام

- Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys & Tutorials*, 15(4), 2070–2090. <https://doi.org/10.1109/SURV.2013.030713.00020>
- Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106, 1–20. <https://doi.org/10.1016/j.eswa.2018.03.050>
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), 1–35. <https://doi.org/10.1145/3469886>
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*.
- Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091–2121. <https://doi.org/10.1109/SURV.2013.032213.00009>
- Zhang, X., & Ghorbani, A. A. (2020). Human factors in cybersecurity: Issues and challenges in big data. In *Security, privacy, and forensics issues in big data* (pp. 66–96). IGI Global. <https://doi.org/10.4018/978-1-5225-9742-1.ch003>