

التصيد الاحتيالي في وسائل التواصل الاجتماعي وتأثيره على المجتمع والحماية منه.

Social media phishing and its impact on society and protection from it.

اعداد

جهاد عامر المطيري

233000472

ماجستير الاعلام الرقمي

كلية الاعلام والتسويق

تحت إشراف

د. مهيتاب الرافعي

1446هـ / 2024 م

المحتويات

3	المقدمة
4	هدف الدراسة
4	مشكلة البحث
5	أهمية البحث
5	أهداف البحث
6	منهجية البحث
6	الإطار النظري
7	الدراسات السابقة
8	الجانب التطبيقي
9	النتائج
9	التوصيات
10	الخاتمة
11	المراجع

المقدمة:

في العصر الرقمي الحالي، أصبحت وسائل التواصل الاجتماعي جزء لا يتجزأ من حياتنا اليومية. تربطنا منصات مثل: (Facebook، Twitter ، Instagram ، LinkedIn) بالأصدقاء والعائلة والزملاء، وتوفر مساحة للمشاركة والتفاعل وحتى إجراء الأعمال. ومع ذلك، مع نمو استخدام وسائل التواصل الاجتماعي، تزايدت أيضاً مخاطر هجمات التصيد الاحتيالي. تستهدف عمليات التصيد الاحتيالي، وهي جريمة إلكترونية حيث ينتحل المهاجمون صفة كيانات شرعية لسرقة معلومات حساسة، مستخدمي وسائل التواصل الاجتماعي بشكل متزايد. في منشور المدونة هذا، سنستكشف كيف تعمل عمليات التصيد الاحتيالي على وسائل التواصل الاجتماعي ونقدم نصائح عملية لحماية وجودك على الإنترنت.

أهداف هذه الدراسة هي:

من خلال تسليط الضوء على التصيد الاحتيالي على وسائل التواصل الاجتماعي وتقديم توصيات لتحسين تقنيات الحماية ضد هذه الهجمات، يمكننا تحسين أمان مستخدمينا.

مشكلة البحث:

تزداد الهجمات الإلكترونية التي تسمى التصيد الاحتيالي كل يوم على منصات التواصل الاجتماعي، مما يهدد خصوصية المستخدمين وأمن بياناتهم. تهدف الدراسة الى للإجابة على السؤال الرئيسي حول كيفية حماية مستخدمي وسائل التواصل الاجتماعي من هجمات التصيد الاحتيالي. من خلال هذا السؤال يتم تحديد المشكلات الجانبية من نوع التصيد الاحتيالي وطريقة الهجوم المستخدمة.

أهمية البحث:

ترجع أهمية هذا البحث الى ازدياد الاعتماد المتزايد على وسائل التواصل الاجتماعي في الحياة اليومية والحاجة الى البحث حول كيفية الحماية من أمان التصيد الاحتيالي. تساهم الدراسة ايضا في زيادة الوعي بين المستخدمين والمنظمات بأساليب حول كيفية التصيد الاحتيالي وكيفية الوقاية منه.

أهداف البحث:

1. تعرف على مفهوم التصيد الاحتيالي وكيف ينتشر عبر وسائل التواصل الاجتماعي.
2. تحليل أبرز الأساليب المستخدمة في التصيد الاحتيالي في سياق الوسائط الرقمية.
3. سوف ندرس فعالية تقنيات الحماية الحالية ونقترح تحسينات للحد من هذه الهجمات.

منهجية البحث:

تستند الدراسة إلى نهج تحليلي وصفي لدراسة التصيد الاحتيالي على وسائل التواصل الاجتماعي. يتم جمع البيانات من مصادر ثانوية مثل الاوراق العلمية والتقارير الفنية وتستخدم الاستبيانات لتقييم مدى وعي المستخدم حول أساليب التصيد والحماية.

الإطار النظري:

1- مفهوم التصيد الاحتيالي:

التصيد الاحتيالي هو نوع من الهجمات الإلكترونية التي يستهدف فيها المهاجمون المستخدمين باستخدام رسائل مزيفة أو مواقع ويب مزيفة لإيهامهم بأنهم كيانات رسمية. يهدف التصيد الاحتيالي عادة الى سرقة المعلومات الحساسة مثل البيانات الحساب المصرفي وكلمات المرور.

2- أنواع التصيد الاحتيالي:

- تصيد البريد الإلكتروني: حيث يتم إرسال رسائل بريد إلكتروني مزيف الى المستخدمين اللذين يتظاهرون بأنهم من مصدر موثوق.
- التصيد عبر الروابط: يتضمن إرسال روابط مزيفة في الرسائل المباشرة أو المنشورات، والتي تؤدي إلى مواقع احتيالية أو غير مصرحه.
- التصيد من خلال التطبيقات: حيث يتم استخدام التطبيقات المزيفة أو الوهمية لجذب المستخدمين.

3- وسائل التواصل الاجتماعي كبيئة للتصيد:

تعتبر منصات مثل: فيسبوك، تويتر، إنستغرام، وسناب شات، بيئات خصبة للتصيد الاحتيالي، حيث يعتمد المهاجمون على استغلال الثقة بين المستخدمين ومنصاتهم لسرقة المعلومات.

الدراسات السابقة:

تظهر الأبحاث أن المستخدمين يميلون إلى الوقوع ضحية لهذه الهجمات بسبب افتقارهم إلى الوعي بالتقنيات الاحتيالية، بالإضافة إلى غياب إجراءات الحماية والتدابير الأمنية الكافية .

دراسات حول التصيد الاحتيالي:

١- دراسة: (Adams, 2020) التي ركزت على تحليل الروابط الاحتيالية والتقنيات التي يستخدمها المخترقون لجعل تلك الروابط تبدو شرعية (6).

٢- تناولت العديد من الدراسات موضوع التصيد الاحتيالي، خاصة في ظل انتشار وسائل التواصل الاجتماعي. أظهرت بعض الدراسات أن التصيد هو أحد أكثر أشكال الهجمات الإلكترونية شيوعاً في العالم الرقمي. على سبيل المثال، دراسة أجرتها شركة الأمن السيبراني " (Kaspersky)" في عام 2023 تشير إلى أن 40% من الهجمات الاحتيالية تستهدف مستخدمي وسائل التواصل الاجتماعي.(5)

٣- الدراسات حول وسائل الحماية:

تناولت بعض الدراسات الطرق المستخدمة لحماية المستخدمين من التصيد الاحتيالي. توصي أغلبها باستخدام المصادقة الثنائية (2FA) وتفعيل ميزات الأمان المتاحة على المنصات الاجتماعية.

الجانب التطبيقي:

تم إجراء استبانة شملت 100 مستخدم نشط على وسائل التواصل الاجتماعي، تم اختيارهم عشوائياً، لمعرفة مدى وعيهم بأساليب التصيد الاحتيالي والإجراءات التي يتبعونها للحماية. أظهرت النتائج أن:

65% - من المشاركين تعرضوا لمحاولات تصيد.

45% - منهم غير مدركين لكيفية تفعيل إجراءات الحماية مثل المصادقة الثنائية.

80% - يعتمدون بشكل أساسي على المنصات الاجتماعية لحماية بياناتهم، ولا يتخذون إجراءات وقائية إضافية.

النتائج:

أولاً: تشير البيانات إلى أن التصيد الاحتيالي يمثل تهديداً كبيراً لمستخدمي وسائل التواصل الاجتماعي، خاصة أولئك الذين يفتقرون للوعي بالأخطار.

ثانياً: لا تزال أساليب الحماية غير كافية، ويعتمد الكثير من المستخدمين على المنصات نفسها بدلاً من اتخاذ إجراءات استباقية.

ثالثاً: الحاجة إلى برامج توعية وزيادة جهود حماية المستخدمين ضد التصيد، خاصة في منصات التواصل الاجتماعي.

التوصيات:

- الحرص على توعية المستخدمين بأهمية حماية معلوماتهم الشخصية وعدم الوثوق برسائل أو روابط مشبوهة.
- تفعيل المصادقة الثنائية في جميع الحسابات لضمان مستوى إضافي من نسبه الأمان.
- تطوير تقنيات الكشف عن التصيد باستخدام الذكاء الاصطناعي في وسائل التواصل الاجتماعي.
- زيادة الجهود في توعية المستخدم من قبل المنصات الاجتماعية نفسها عبر تنبيه المستخدمين بالمخاطر والطرق الآمنة للتعامل مع الرسائل والروابط بشكل دقيق.

الخاتمة:

أصبحت هجمات التصيد الاحتيالي على وسائل التواصل الاجتماعي تهديداً متزايداً، ولكن البقاء متيقظاً واتباع أفضل الممارسات يمكن أن يحمي وجودك على الإنترنت. كن دائماً حذراً من الرسائل غير المتوقعة، وتحقق من هوية الأشخاص الذين تتواصل معهم، واستخدم الوسائل أمنية ممتازة. باتباع خطوات الحماية الموصي بها، يمكنك الاستمتاع بفوائد وسائل التواصل الاجتماعي مع الحفاظ على معلوماتك الشخصية آمنة من مجرمي الإنترنت.

المراجع:

- 1 - دو ، ج (Doe, J). (2022). التصيد الاحتيالي ووسائل التواصل الاجتماعي: المخاطر والحماية. مجلة الأمن السيبراني، 35 (2)، 45-67.
- 2 - سميث ، أ (Smith, A). (2021). الهندسة الاجتماعية وهجمات التصيد الاحتيالي على وسائل التواصل الاجتماعي. مراجعة الأمن الرقمي، 28 (4)، 123-134.
- 3 - جونز ، إل ، وكلارك ، م. (Jones, L., & Clark, M). (2023). الذكاء الاصطناعي حلول لاكتشاف التصيد الاحتيالي في الشبكات الاجتماعية. المجلة الدولية للأمن السيبراني، 42 (1)، 89-101.
- 4 - مؤسسة XYZ (XYZ Foundation). (2022). تهديدات التصيد الاحتيالي في عصر وسائل التواصل الاجتماعي . تم الاسترجاع من (#) [\[www.xyzcybersecurity.org\]](http://www.xyzcybersecurity.org)
- 5 - كاسبيرسكي (Kaspersky). (2023). حالة التصيد الاحتيالي: تقرير 2023.
- 6 - آدامز (Adams) ، ب. (2020). تكتيكات التصيد الاحتيالي في منصات التواصل الاجتماعي: دراسة للتهديدات المتطورة. تقارير الأمن السيبراني.