

تسليم 5 لمقرر قضايا بحثية 1

إعداد: عبدالله نصر الدين
الرقم الاكاديمي: 251001251

تسليم 5



التصيد الاحتيالي في ظل التطور التقني

تسليم ورقة بحثية 5

المصدر: "مجلة الدراسات القانونية والاقتصادية"
[الرابط: انقر هنا](#)



- ✓ تعريف التصيد الاحتيالي: هو أحد أكثر أنواع الهجمات السيبرانية انتشاراً، حيث يعتمد على خداع المستخدمين وإقناعهم بمشاركة بياناتهم الشخصية مثل كلمات المرور، الحسابات البنكية، والمعلومات السرية.
- ✓ أهميته: 90% من الهجمات السيبرانية تبدأ بهجمات تصيد
- ✓ هدف البحث: فهم استراتيجيات التصيد وتحليل سبل الوقاية منه.

تسليم

05

العنوان ومدى جاذبيته

- العنوان واضح، مباشر، ويعكس مضمون الدراسة.
- يشير إلى موضوع حديث ومهم في مجال الأمن السيبراني.
- يحتوي على كلمات مفتاحية مهمة مثل "التصيد الإلكتروني" و"كيف يقع المستخدمون ضحية له"، مما يجعله ملفتًا ومناسبًا للبحث الأكاديمي.

يمكن تحسينه ليشمل جانب الحلول، مثل:
"التصيد الإلكتروني: كيف يقع المستخدمون ضحية له؟ وأفضل الطرق لمكافحته".

تسليم

05

المقدمة ومدى وضوحها

- التصيد الإلكتروني هو هجوم يستخدم أساليب الهندسة الاجتماعية لخداع المستخدمين وسرقة بياناتهم.
- أصبح التصيد يمثل 90% من الهجمات السيبرانية عالميًا.
- يهدف هذا البحث إلى تحليل أساليب التصيد، التحديات التي تواجه مكافحته، والحلول الممكنة لحماية المستخدمين.

تسليم

05

مشكلة الدراسة

مع التطور المستمر للتكنولوجيا، أصبحت أساليب التصيد الاحتيالي أكثر تطورًا، ولم يعد المستخدم العادي قادرًا على التمييز بسهولة بين المواقع الحقيقية والمزيفة.

كيف تطورت أساليب التصيد الإلكتروني، وما هي أفضل الاستراتيجيات لمكافحته؟

تسليم

05

أهمية الدراسة

الأهمية النظرية:

- تحليل تطور التصيد الإلكتروني وأهم أساليبه. 
- استكشاف العلاقة بين الهندسة الاجتماعية والتصيد. 

الأهمية التطبيقية:

- تقديم حلول وقائية للحد من خطر التصيد. 
- المساهمة في رفع مستوى الوعي الأمني لدى المستخدمين. 

أهداف الدراسة

- ✓ تحليل أبرز أساليب التصيد الإلكتروني الحديثة.
- ✓ دراسة التحديات التي تواجه مكافحة التصيد.
- ✓ تقديم حلول واستراتيجيات تقنية وقانونية للحد من مخاطره.

فرضيات الدراسة

- ◆ هناك علاقة بين ضعف الوعي الأمني وزيادة التصيد.
- ◆ استخدام الذكاء الاصطناعي يزيد من تعقيد التصيد.

📖 دراسة Vayansky & Kumar (2018): التصيد هو التهديد
السيبراني الأول عالميًا.

📖 دراسة Alkhalil et al. (2021): الهندسة الاجتماعية تلعب دورًا
رئيسيًا في نجاح التصيد.

📌 ما تضيفه دراستنا:

- ✓ تحليل تأثير التزييف العميق والذكاء الاصطناعي في تطوير التصيد.
- ✓ تقديم مقارنة بين استراتيجيات مكافحة التصيد عالميًا.

الدراسات السابقة

76% من الشركات تعرضت لهجوم تصيد إلكتروني
(CISA 2023).

30% من المستخدمين ينقرون على روابط تصيد دون تدقيق
(Microsoft 2023).

25% من الضحايا يستخدمون نفس كلمة المرور في مواقع
متعددة.



تسليم
05

التحليل الإحصائي

تسليم

05

دراسة حالة-التصيد الإلكتروني في جامعة ميدأوشن



الطلاب الأعزاء،

لوحظ في الآونة الأخيرة انتحال أحد الأشخاص صفة موظف في إدارة القبول والتسجيل لجامعة ميدأوشن، مدعيًا صلاحيات تخوله إجراء خصومات للطلاب عند التسجيل.

وعليه، نؤكد أن وسائل التواصل الحصرية مع الجامعة هي:

- التذاكر.

- حساب الطالب على المنصة الأكاديمية SIS، أو حسابه على تطبيق الجوال.

- موقع الجامعة الرسمي للتسجيل عبره.

كما نلفت انتباهكم إلى أنه لا توجد أي مجموعات رسمية تابعة للجامعة على تطبيقات التواصل (WhatsApp, Telegram)، وأن رقم التواصل المدرج في النظام هو الرقم الرسمي الوحيد المعتمد

فيما عدا المذكور آنفًا، نحن لسنا مسؤولين عن تبعاته.

شاكرين لكم تفهمكم وتعاونكم.

كيف حدث التصيد؟

- انتحل المهاجم صفة موظف جامعي لخداع الطلاب.
- طلب منهم مشاركة بياناتهم عبر بريد إلكتروني احتيالي.
- تدخلت الجامعة وأصدرت تحذيرًا رسميًا.

النتائج والتوصيات

- ✓ تعزيز الوعي الأمني: تدريب الموظفين والمستخدمين.
- ✓ استخدام المصادقة الثنائية لحماية الحسابات.
- ✓ تطوير تقنيات ذكاء اصطناعي للكشف عن التصيد.
- ✓ تحديث التشريعات والقوانين لمكافحة الاحتيال الإلكتروني.

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060.
- Vayansky, I., & Kumar, S. (2018). Phishing–Challenges and solutions. *Computers & Security*, 73, 109-121.
- Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation.
- Anti-Phishing Working Group (APWG). (2023). *Phishing activity trends report – Q2 2023*.

المراجع الأكاديمية



Thank You