

المنهج الاستقراري في البحث العلمي مهارات بحثية 1

إعداد: عبدالله نصر الدين
الرقم الاكاديمي: 251001251

تسليم 3



عنوان البحث: الثقافة التنظيمية ودورها في تعزيز الأمن السيبراني

مهارات بحثية 1

إعداد
عبدالله نصرالدين

إعداد الورقة البحثية: تقوى محمد عيس وي
تم نشره بواسطة: جامعة مطروح، كلية السياحة والفنادق
رابط المصدر: [الرابط هنا](#)



تواجه المؤسسات في العصر الرقمي تحديات متزايدة في مجال الأمن السيبراني، حيث لم يعد الاعتماد على الحلول التقنية كافياً. أصبحت الثقافة التنظيمية تلعب دوراً رئيسياً في حماية الأنظمة والمعلومات من الهجمات السيبرانية.

تهدف هذه الدراسة إلى تحليل تأثير الثقافة التنظيمية على الأمن السيبراني، واستكشاف العوامل التي تؤثر على نجاح تبني سياسات أمنية فعالة داخل المؤسسات.

تسليم

03

أهداف البحث

1. تحليل العلاقة بين الثقافة التنظيمية ومستوى الأمن السيبراني في المؤسسات.
2. استكشاف دور القيادة الإدارية في ترسيخ ثقافة الأمن السيبراني.
3. دراسة أثر وعي الموظفين وثقافة المؤسسة في تقليل المخاطر السيبرانية.
4. اقتراح استراتيجيات لتعزيز الثقافة التنظيمية بما يدعم ممارسات الأمن السيبراني.

تسليم

03

أهمية البحث

- **حماية الأصول المعلوماتية:** فهم تأثير الثقافة التنظيمية يساعد في تعزيز سياسات الأمن السيبراني، مما يحمي البيانات الحساسة من التهديدات المحتملة.
- **رفع كفاءة الموظفين:** التوعية الأمنية تقلل من الأخطاء البشرية التي قد تؤدي إلى اختراقات سيبرانية (mahmudi, 2019).
- **تحسين سمعة المؤسسة:** المؤسسات التي تدمج ثقافة الأمن السيبراني في بيئتها تحقق ثقة أعلى من العملاء والشركاء.
- **الامتثال للمعايير الدولية:** تساهم الثقافة التنظيمية القوية في تحقيق الامتثال للتشريعات والسياسات الأمنية المطلوبة عالميًا.

تسليم

03

المنهجية البحثية

يعتمد البحث على المنهج الاستكشافي، نظرًا لكونه الأكثر ملاءمة لدراسة تأثير العوامل البشرية والثقافية على الأمن السيبراني. سيتم استخدام الطرق التالية لجمع البيانات:

1 **المقابلات المعمقة:** مع خبراء الأمن السيبراني ومديري الموارد البشرية لاستكشاف تأثير الثقافة التنظيمية على سياسات الأمن.

2 **الاستبيانات:** جمع بيانات من الموظفين في مختلف المؤسسات لقياس مستوى الوعي الأمني، وسيتم تحليلها باستخدام برنامج SPSS لاستخلاص نتائج دقيقة حول تأثير الثقافة التنظيمية على الأمن السيبراني.

3 **دراسة الحالة:** تحليل مؤسسات طبقت ممارسات ناجحة في دمج الثقافة التنظيمية مع الأمن السيبراني.

من المتوقع أن تظهر الدراسة أن المؤسسات التي لديها ثقافة تنظيمية قوية في الأمن السيبراني تحقق نسبة أقل من الاختراقات الأمنية مقارنة بالمؤسسات التي تفتقر إلى وعي وتدريب أمني كافٍ. كما يُتوقع أن يكون للدعم الإداري والسياسات الواضحة دور حاسم في تعزيز الأمن السيبراني داخل المؤسسات. يتوقع أن يساهم هذا البحث في تطوير سياسات أمنية أفضل داخل المؤسسات، مما قد يؤدي إلى انخفاض عدد الهجمات السيبرانية بنسبة 30% في الشركات التي تتبنى ممارسات أمنية قوية (Smith, 2022).

نتائج متوقعة

على الرغم من أهمية الدراسة، هناك بعض التحديات التي قد تؤثر على دقة النتائج، منها:

✓ حجم العينة المحدود، حيث سيتم الاعتماد على بيانات من عدد معين من المؤسسات فقط، مما قد يؤثر على قابلية تعميم النتائج على جميع القطاعات.

✓ إمكانية التحيز في الاستبيانات نتيجة لاختلاف وعي وثقافة الموظفين المشاركين.

✓ عدم القدرة على التحكم في جميع المتغيرات، حيث يمكن أن تؤثر عوامل أخرى غير الثقافة التنظيمية على الأمن السيبراني.

حدود البحث

- ✓ تصميم برامج تدريب دورية تشمل محاكاة للهجمات السيبرانية لتعزيز الوعي الأمني.
- ✓ تفعيل سياسة "الأبواب المفتوحة" للإبلاغ عن التهديدات دون خوف من العقوبات.
- ✓ دمج الأمن السيبراني في استراتيجية المؤسسة بحيث يصبح جزءًا من هوية المؤسسة وثقافتها.
- ✓ تعزيز المساءلة الفردية بحيث يكون لكل موظف دور واضح في حماية البيانات والمعلومات.
- ✓ إدراج الأمن السيبراني ضمن معايير تقييم أداء الموظفين.



تسليم
03

التوصيات

توضح هذه الدراسة أهمية دمج الثقافة التنظيمية في استراتيجيات الأمن السيبراني للمؤسسات. من خلال التركيز على التوعية والتدريب والدعم الإداري، يمكن للمؤسسات تقليل المخاطر السيبرانية وتعزيز مستوى الحماية ضد الهجمات المتزايدة في العصر الرقمي. بناءً على هذه النتائج، توصي الدراسة المؤسسات بتبني سياسات أمنية أكثر شمولاً، تشمل تدريباً دورياً للموظفين، بالإضافة إلى إدراج الأمن السيبراني ضمن معايير تقييم الأداء المؤسسي.



تسليم
03

الخاتمة

- Smith, J. (2022). Organizational Culture and Cybersecurity Practices. Cybersecurity Journal, 10(2), 45-67.
- Mahmoudi, A. (2019). Cybersecurity Awareness in Organizational Culture. International Journal of Security, 15(3), 89-102.
- Wang, X., & Johnson, T. (2021). Cybersecurity Culture in Organizations: Strategies and Challenges. International Journal of Cybersecurity Research, 14(3), 88-102.
- National Institute of Standards and Technology (NIST). (2020). Cybersecurity Framework Implementation Guide. Retrieved from NIST.gov
- ISO/IEC 27001 Standard. (2021). Information Security Management Systems - Requirements. International Organization for Standardization.

المراجع الأكاديمية



Thank You