ملخص البحــث رقـــم (8)

السيد الأستاذ الدكتور/ مقرر اللجنة العلمية الدائمة لترقية الأساتذة والأساتذة المساعدين للحاسبات والمعلومات

تحية طيبة وبعد –احيط سيادتكم علما بان البحث رقم 8 بياناتة كالتالي

عنوان البـــــحث باللغة الانجليزية:

Machine Learning Techniques for Detecting Phishing URL Attacks

عنوان البـــــحث باللغة العربية

تقنيات التعلم الآلي لاكتشاف هجمات عناوين URL الخادعة

اسماء المؤلفين:

Diana T. Mosa 1,2, Mahmoud Y. Shams3,*, Amr A. Abohany2, El-Sayed M. El-kenawy4, M. Thabet5

مكان النشر و تاريخه:

Computers, Materials & Continua (CMC), December 2022

ملخص البـــــحث باللغة العربية :

تعتبر الهجمات الإلكترونية حاسمة ومدمرة لجميع قطاعات الصناعة. إنها تؤثر على الهندسة الاجتماعية من خلال السماح بالوصول غير المعتمد إلى جهاز كمبيوتر شخصي (PC) يكسر النظام التالف ويهدد البشر. يتطلب الدفاع عن الأمن فهم طبيعة الهجمات الإلكترونية ، لذلك يصبح المنع سهلاً ودقيقًا من خلال اكتساب المعرفة الكافية حول السمات المختلفة للهجمات السيبرانية. يقترح الأمن السيبراني الإجراءات المناسبة التي يمكنها التعامل مع الهجمات وصدها. هجوم التصيد هو إحدى الجرائم الإلكترونية التي يتبع فيها المستخدمون رابطًا إلى مواقع ويب غير قانونية تقنعهم بالكشف عن معلوماتهم الخاصة. أحد تحديات الأمان عبر الإنترنت هو العدد الهائل من المعاملات اليومية التي تتم عبر مواقع التصيد الاحتيالي. نظرًا لأن الأمن السيبراني له أولوية لجميع المنظمات ، تعتبر مخاطر الأمن السيبراني جزءًا من عملية إدارة المخاطر في المؤسسة. تقدم هذه الورقة مسحًا لمختلف مناهج التعلم الآلي الحديثة التي تتعامل مع مشكلات التصيد الاحتيالي وتكشف بدقة عالية الجودة عن هجمات التصيد

المختلفة. تم استخدام مجموعة بيانات تتكون من أكثر من 11000 موقع ويب من مجموعة بيانات Kaggle ودراسة تأثير 30 ميزة لموقع الويب وعلامة التصنيف الناتجة التي تشير إلى ما إذا كان موقع ويب للتصيد الاحتيالي أم لا (1 أو -1). علاوة على ذلك ، حددنا مصفوفات الارتباك لنماذج التعلم الآلي: الشبكات العصبية (NN) و Naïve Bayes و Adaboost ، وأشارت النتائج إلى أن الدقة التي تم تحقيقها كانت 90.23٪ و 92.97٪ و 95.43٪ على التوالي.