SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.04 NO. 3 2025
DOI: 10.51984/SUCP.V4I3.4126

وقائع مؤتمرات جامعة سبها
Sebha University Conference Proceedings

Confrence Proceeeding homepage: http://www.sebhau.edu.ly/journal/CAS

تحليل أمان الشبكات الجامعية باستخدام Kali Linux: دراسة تطبيقية مع مقترح Naive Bayes

حسن عبدالله أبكر

مدرسة الدكتوراه بجامعة الملك فيصل بتشاد، جمهورية تشاد

الملخص

شهد التعليم العالي تحولًا رقميًا متسارعًا جعل الجامعات أكثر عرضة للتهديدات السيبرانية، خصوصًا عبر الشبكات اللاسلكية والأنظمة السحابية. تهدف هذه الدراسة إلى تقييم أمني تطبيقي لجامعة الملك فيصل في تشاد من أجل تحديد الثغرات التقنية والبشرية. استخدمت الدراسة أدوات **Kali Linux** (مثل Aircrack-ng و Airodump-ng و Social Engineering Toolkit) إلى جانب التحليلات الإحصائية (ANOVA، و اختبارWelch T، واختبار كاي مربع). شملت العينة 634 جهازًا موزعة على أربع فئات أكاديمية: أعضاء هيئة التدريس، وطلاب هندسة الحاسوب، وطلاب التخصصات العلمية، وطلاب التخصصات الأدبية. أظهرت النتائج اختراق 51% من الأجهزة، حيث كان طلاب التخصصات الأدبية الأكثر عرضة، في حين سجّل أعضاء هيئة التدريس وطلاب هندسة الحاسوب أقل نسب اختراق. كما كشفت النتائج عن علاقة ذات دلالة إحصائية بين الفئة الأكاديمية ومستوى القابلية للهجمات، إلى جانب ضعف في إعدادات الشبكات. توصي الدراسة بتعزيز السياسات المؤسسية، وتكثيف التدريب على الوعي السيبراني، وتحديث البنية التكنولوجية. كما تقترح توظيف خوارزميات الذكاء الاصطناعي مثل **Naive Bayes** في أبحاث مستقبلية لتطوير أنظمة ذكية للكشف المبكر عن التهديدات. ومع أهميتها العملية، تقتصر الدراسة على مؤسسة واحدة وفترة رصد قصيرة مدتها خمسة أيام.

الكلمات المفتاحية:

الأمن السيبراني
الاختراق الأخلاقي
اختبار الاختراق
الخوارزميات الذكية
التصيد الاحتيالي
الهندسة الاجتماعية
كالي لينكس
خوارزمية Naïve Bayes

University Network Security Analysis Using Kali Linux:An Applied Study and a Naive Bayes Proposal

Hassan Abdoulaye Abakar

Doctoral School, King Faisal University in Chad, Republic of Chad

Keywords:

CyberSecurity
Ethical hacking
Penetration testing
Intelligent algorithms
Awareness,
Social engineering
Network security
Kali Linux,
Naive Bayes Algorithm

A B S T R A C T

The rapid shift toward digital transformation in higher education has exposed universities to escalating cybersecurity threats, particularly through wireless and cloud-based systems. This study conducts an applied security assessment of King Faisal University in Chad to identify technical and human vulnerabilities. Using Kali Linux tools (Aircrack-ng, Airodump-ng, Social Engineering Toolkit) combined with statistical analysis (ANOVA, Welch's T-test, chi-square), the research tested 634 devices across four academic groups: faculty, computer engineering students, scientific disciplines, and humanities disciplines. Results showed that 51% of devices were compromised, with humanities students being the most vulnerable and faculty/computer engineering students the least. Findings revealed a statistically significant link between academic group and susceptibility, alongside weaknesses in network configurations. The study recommends strengthening institutional policies, enhancing awareness training, and upgrading technological infrastructure. Future research should integrate artificial intelligence techniques, such as Naive Bayes classifiers, for intelligent early detection systems. Despite its practical value, the study is limited to a single institution and a five-day observation period.

1. المقدمة

يشهد العالم اليوم تحولًا رقميًا متسارعاً يفرض على المؤسسات التعليمية في الدول النامية تحديات أمنية متزايدة، تنبع أساسًا من محدودية الموارد

*Corresponding author:
E-mail addresses: hassan_kaly@hotmail.com

Article History : Received 20 February 2025 - Received in revised form 01 September 2025 - Accepted 07 October 2025

التقنية، وقلة الكوادر المتخصصة، وضعف وعي المستخدمين بالتهديدات الإلكترونية الجنفاوي (2021). وتُعد الجامعات من أكثر البيئات عرضة للهجمات السيبرانية نظرًا لتعدد المستخدمين، وتنوع أجهزتهم، واعتمادهم المتنامي على الشبكات اللاسلكية والتطبيقات السحابية. وقد أظهرت دراسات سابقة (Alenezi, 2021؛ Zhang & Others, 2022) أن غياب السياسات الأمنية الفعّالة، وضعف برامج التدريب والتوعية المستمرة، يجعل هذه المؤسسات أكثر هشاشة أمام هجمات متنوعة، من بينها التصيد الاحتيالي، وكسر كلمات المرور، والهندسة الاجتماعية.

انطلاقًا من هذه التحديات، جاءت هذه الدراسة لتسد فجوة معرفية متعلقة بأمن الشبكات والأجهزة في البيئات الجامعية الإفريقية، وذلك من خلال دراسة تطبيقية على جامعة الملك فيصل في تشاد. وتعتمد الدراسة على تنفيذ اختبارات اختراق عملية باستخدام أدوات Kali Linux، إلى جانب تحليل مستوى الوعي الأمني لدى مختلف الفئات داخل الجامعة.

أهداف البحث

1. تقييم مستوى أمان الشبكات والأجهزة في جامعة الملك فيصل بتشاد.
2. قياس مستوى وعي المستخدمين واستجابتهم لمحاولات التصيد والهندسة الاجتماعية.
3. تحديد أبرز الثغرات الأمنية التقنية والبشرية التي تهدد البنية الرقمية للمؤسسة.
4. اقتراح حلول تقنية وسلوكية لتعزيز الحماية، بما في ذلك الاستفادة من الخوارزميات الذكية مثل Naive Bayes كاتجاه مستقبلي.

أسئلة البحث

1. ما هي أبرز نقاط الضعف التقنية والبشرية في الشبكات الجامعية قيد الدراسة؟
2. كيف يختلف مستوى الوعي الأمني بين فئات المستخدمين (طلاب، أساتذة، إداريين)؟
3. ما مدى فعالية محاكاة هجمات التصيد والاختراق في الكشف عن الثغرات؟
4. كيف يمكن توظيف الذكاء الاصطناعي(Naive Bayes) لتقليل المخاطر الأمنية في المؤسسات التعليمية؟

مراجعة الأدبيات:

شهدت السنوات الأخيرة اهتمامًا متزايدًا بدراسة قضايا أمن المعلومات في البيئات التعليمية، لاسيما مع التوسع الكبير في استخدام الشبكات اللاسلكية ومنصات التواصل الرقمي داخل الجامعات. فقد أشار Alenezi (2021)، إلى أن التحول الرقمي المتسارع في مؤسسات التعليم العالي غالبًا ما يترافق مع ثغرات تقنية حرجة ناجمة عن ضعف السياسات الأمنية ونقص الكفاءات المتخصصة. وفي السياق نفسه، أكد Zhang & Others (2022) أن توظيف الخوارزميات الذكية مثل Naive Bayes وSVM يعزز من كفاءة أنظمة الكشف المبكر عن التهديدات السيبرانية، الأمر الذي يجعلها أدوات واعدة لتعزيز منظومات الحماية الرقمية. وقد أشار الحسيني (2022) أيضاً إلى أن التحول الرقمي في الجامعات العربية ما يزال يواجه عقبات تنظيمية وبشرية، وهو ما ينعكس على ضعف تبني سياسات أمنية فعّالة. ويدعم Marks (2020) هذا الاتجاه من خلال وضع إطار لتقييم نضج التحول الرقمي في مؤسسات التعليم العالي.

أما في جانب الهندسة الاجتماعية، فقد أوضح Hadnagy (2018) أن العامل البشري يظل الحلقة الأضعف في منظومة الدفاعات الأمنية، حيث يمكن استغلال الثقة والعوامل العاطفية لخداع الضحايا وحملهم على النقر على روابط ضارة أو تسريب بيانات حساسة. وتؤكد دراسات عربية مثل دراسة العتيبي (2022) هذه النتيجة، إذ أظهرت أن ضعف الوعي الأمني بين الطلاب والموظفين يجعل الجامعات بيئة خصبة للهجمات المعتمدة على الخداع البشري. وتتوافق هذه النتيجة مع ما بينته حمدان (2021) من محدودية وعي الأفراد بمخاطر الأمن السيبراني في البيئات الأسرية والتعليمية.

وفيما يتعلق بتطبيقات اختبارات الاختراق، بيّن النوري (2022) فعالية الأدوات مفتوحة المصدر مثل Kali Linux في اكتشاف الثغرات في الشبكات اللاسلكية، مشددًا على أهمية دمج هذه الاختبارات ضمن السياسات المؤسسية للأمن السيبراني. ومن جانب آخر، ناقشت بغدادي (2024) دور الذكاء الاصطناعي كخيار استراتيجي لتعزيز قدرة المؤسسات التعليمية على مواجهة التهديدات المعلوماتية المتزايدة.

وعلى الرغم من هذه الجهود البحثية، ما تزال هناك فجوة واضحة في الأدبيات، خصوصًا فيما يتعلق بندرة الدراسات التطبيقية في الجامعات الإفريقية، ولا سيما في البيئات محدودة الموارد مثل تشاد. فمعظم الدراسات السابقة ركزت على مؤسسات في الدول المتقدمة أو في منطقة الشرق الأوسط، بينما تفتقر إفريقيا جنوب الصحراء إلى أبحاث ميدانية شاملة تدمج بين التجارب العملية لاختبارات الشبكات، وتحليل سلوك المستخدمين، واقتراح الخوارزميات الذكية كحلول مستقبلية. ومن هنا تبرز أهمية هذه الدراسة التي تسعى إلى تقديم نموذج تطبيقي متكامل يجمع بين التحليل التجريبي والمقاربة المستقبلية المعتمدة على الذكاء الاصطناعي لمعالجة هذه الفجوة.

2. منهجية الدراسة:

اعتمدت هذه الدراسة مقاربة منهجية تجمع بين التحليل النظري والتجريب العملي، وذلك على النحو الآتي:

1.2. المنهج التحليلي النظري (Literature-based Analysis):

تم إجراء مراجعة منهجية للأدبيات الحديثة في مجالات الأمن السيبراني، اختبارات الاختراق، والخوارزميات الذكية، مع التركيز على الدراسات التي تناولت شبكات الجامعات وأساليب التصيد والهندسة الاجتماعية. ساعد هذا الإطار النظري في صياغة الفرضيات وتحديد محاور الدراسة.

2.2. المنهج التطبيقي (Experimental Method):

أُجريت اختبارات اختراق عملية داخل شبكة جامعة الملك فيصل بتشاد، بعد الحصول على الموافقات الرسمية، وشملت:

- اختبار اختراق الشبكات اللاسلكية: باستخدام أدوات متخصصة في Kali Linux (Aircrack-ng,) للكشف عن الثغرات في أنظمة التشفير والمصادقة.
- محاكاة هجمات التصيد الإلكتروني للاجهزة: من خلال تصميم حملات تجريبية وقياس وعي المستخدمين وتحليل استجاباتهم. عبر استخدام Social Engineering Toolkit (SET)
- تحليل الثغرات الأمنية: باستخدام أدوات مثل Zphisher لمحاكاة هجمات انتحال الهوية عبر الروابط المزيفة.

شملت العينة 634 مستخدمًا من أساتذة، طلاب، وإداريين. وتم توثيق الاستجابات ونسب النجاح في محاولات الاختراق المختلفة

3.2. التحليل الإحصائي (Statistical Analysis):

تم استخدام برنامج SPSS لإجراء التحليل الكمي للبيانات، حيث طُبّقت:

اختبار ANOVA أحادي الاتجاه لمقارنة الفروق بين الفئات.

اختبار T-test لمقارنة متوسطات مجموعتي الطلاب مقابل باقي المستخدمين.

اختبار مربع كاي (Chi-Square Test) للكشف عن العلاقة بين الفئة الأكاديمية واحتمالية الاختراق.

3.2.المقترح المستقبلي (Future Proposal):

لم يتم تطبيق خوارزمية Naive Bayes في هذه التجربة الميدانية، وإنما طُرحت كخيار بحثي مستقبلي لتطوير نظام ذكي للتصنيف الآلي للرسائل الإلكترونية والروابط المشبوهة. يهدف هذا المقترح إلى استكمال العمل الميداني الحالي بآلية تقنية مستدامة.

3. الإطار النظري:

1.3.كالي لينكس وأدوات الاختراق: Kali Linux هو نظام تشغيل مفتوح المصدر مبني على توزيعة Debian، يحتوي على أكثر من 600 أداة أمنية موجهة لاختبار اختراق الأنظمة والشبكات (Kali Linux Docs). تشمل هذه الأدوات: Aircrack-ng لكسر تشفير شبكات الواي فاي، Metasploit لاستغلال الثغرات في الأنظمة، وWireshark لتحليل حركة مرور البيانات في الشبكات. هذه الأدوات تتيح لمحترفي الأمن السيبراني إجراء اختبارات واقعية لتحديد مدى جاهزية البنية التحتية الرقمية للمؤسسة ضد الهجمات.

2.3.الهندسة الاجتماعية: تُعد الهندسة الاجتماعية من أكثر الأساليب فاعلية في الهجمات السيبرانية الحديثة، حيث يتم استغلال العامل البشري بدلاً من نقاط الضعف التقنية (Hadnagy, 2018). تشمل هذه الأساليب التصيد الاحتيالي عبر البريد الإلكتروني أو رسائل التواصل الاجتماعي، وانتحال هوية مسؤولي النظام. إن ضعف الوعي الأمني يشكل عاملاً رئيسيًا في نجاح هذا النوع من الهجمات. (العتيبي، 2022).

تعتمد الهندسة الاجتماعية على:

الخداع النفسي : التصيد، انتحال الشخصية

الثقة المبنية على معلومات: التظاهر بمعرفة معلومات شخصية

الإلحاح العاطفي :خلق حالة طوارئ مزيفة

مميزاتها:

- ✓ فعالة ضد أي نظام (حتى المحمي تقنياً).
- ✓ لا تحتاج لمهارات برمجية عالية.
- ✓ نتائج سريعة مع ضحايا غير مدربين.

عيوبها:

- ✓ تعتمد على قابلية الضحية للخداع.
- ✓ قد تكون غير قانونية بدون إذن.
- ✓ محدودة التأثير ضد المدركين للخطر.

3.3. **خوارزمية** Naive Bayes: تعتبر من الخوارزميات الذكية قادرة على التعلم من البيانات وتحليل الأنماط واكتشاف السلوك غير الطبيعي. حيث تعتمد على الاحتمالات لتصنيف الرسائل الإلكترونية.(Saxe & Berlin, 2015؛ Salloum & others, 2021). حيث استخدمت خوارزمية **Naive Bayes** في العديد من المجالات التطبيقية، ومنها المجال الطبي، حيث أثبتت فعاليتها في تصنيف البيانات وتحقيق نسب دقة تجاوزت 85% في التنبؤ بالأمراض (بغدادي، 2024؛ باحثون آخرون، 2023). وانطلاقًا من هذه النجاحات، تقترح هذه الدراسة على الخوارزمية نفسها لتصنيف الرسائل الإلكترونية والروابط الشبكية داخل بيئة المؤسسات التعليمية. وقد ساعد هذا الدمج بين التجارب السابقة والتطبيق الحالي في تقديم نموذج متكامل يمكن توظيفه في تطوير أنظمة الإنذار المبكر ضد الهجمات السيبرانية داخل المؤسسات التعليمية.

ورغم أهمية خوارزمية Naive Bayes في مجال الكشف المبكر عن الهجمات السيبرانية، لم يتم تطبيقها فعليًا في هذه الدراسة نظرًا لقيود البيانات وحجم العينة، وقصر الفترة الزمنية الميدانية، إضافة إلى محدودية البنية التحتية التقنية في البيئة الجامعية قيد الدراسة. وعليه، تم الاقتصار على تحليل وصفي وإحصائي للثغرات الأمنية والوعي البشري، مع الإشارة إلى Naive Bayesكاتجاه بحثي واعد لأعمال مستقبلية أكثر شمولًا

4. الإطار العملي:

البيئة المستهدفة: تمثلت البيئة التطبيقية في شبكة جامعة الملك فيصل بتشاد، والتي تضم آلاف المستخدمين من طلاب وموظفين وإداريين وأعضاء هيئة تدريس. الشبكة تتضمن من عدة نقاط وصول لاسلكية، بالإضافة إلى استخدام واسع النطاق للبريد الإلكتروني ومنصات التراسل مثل واتساب على شكل مجموعات تراسل إداري وإعلانات للطلاب وكما تعتمد على منظومة مركزية للتسجيل الالكتروني تعمل في شبكة انترانت. حيث تمت عملية التجارب في البيئة الحقيقية بعد موافقة وعلم الجهات المختصة بذلك.

وتناول الجانب التطبيقي في شكل ثلاث سيناريوهات الأولى للشبكة والثانية لاختراق الأجهزة عبر البريد الالكتروني وعبر الروابط المشبوهة والثالثة لتحليل الثغرات الأمنية.

السيناريو الاول: اختبار اختراق الشبكة اللاسلكية.

- الأدوات المستخدمة: مجموعة Aircrack-ng ضمن منصة (Kali Linux Docs).

- الطريقة:

اعتراض وحزم المصافحة (handshake) للشبكة اللاسلكية باستخدام Airodump-ng.

تحليل نقاط الضعف في انظمة التشفير والمصادقة.

جمع المعلومات حول البنية التحتية للشبكة المستهدفة.

معلومات حول الشبكة المستهدفة عبارة عن شبكة محلية مخصصة للأعمال الإدارية وعبر راوتر محمي ومشفر حيث تم اعطاء الاذن لتجربة الاختراق على راوتر واحد فقط وتمت التجربة لمدة 5 أيام بداية الاختبار **يوم 07 – 04 – 2025 م** الى 12-04-2025م.

الشبكة المستهدفة: Askaw

BSSID: C0:C1:C0:23:0F:A9 :العنوان الفريد لنقطة الاتصال BSSID

القناة(CH): 11

نوع التشفير:WPA2-PSK (AES-CCMP)

كلمة السر المكتشفة: ✅ 11167844

مدة الاختبار: 5-2~ :دقائق

جدول رقم (2) يوضح الأدوات المستخدمة في الاختبار

الأداة	الوظيفة
airodump-ng	مراقبة الشبكات، التقاط الHandshake ، جمع بيانات البث اللاسلكي
aireplay-ng	تنفيذ هجمات إعادة المصادقة (Deauthentication) لاجبار الأجهزة على إعادة

	الاتصال
aircrack-ng	كسر كلمة المرور باستخدام ملف wordlist على ملفhandshake

حيث يوضح الأدوات التي استخدمت خلال تجارب الاختراق ووظائفها .

1.4. إجراءات اختبار اختراق الشبكة الداخلية الواي فاي :

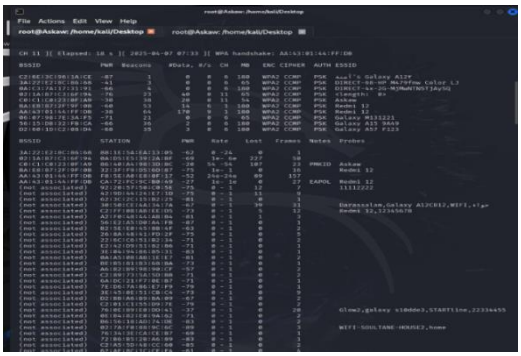
أولاً: مراقبة الشبكة وجمع المعلومات:

تم استخدام الأمر:

```
bash
CopyEdit
airodump-ng wlan0
```

الهدف منه هو التعرف على الشبكات المتاحة.

تم رصد الشبكة "Askaw" بقوة إشارة 30- dBm وهو ما يدل على قرب الجهاز المستهدف. كما هو موضح في الشكل رقم (2).



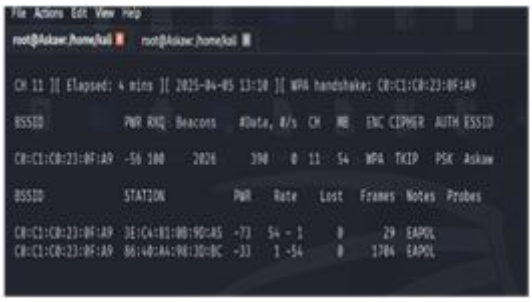
الشكل رقم (2): يوضح الشبكات المتاحة

ثانياً: التقاط الـ:WPA Handshake

تم توجيه الأداة إلى BSSID الخاص بالشبكة مع تحديد القناة:

```
bash
CopyEdit
airodump-ng -w attackmoussa -c 11 --bssid
C0:C1:C0:23:0F:A9 wlan0
```

الشكل رقم(3) يوضح ذلك:



الشكل رقم(3): التقاط الـWPA Handshake

تمت ملاحظة ظهور رسالة:

```
ruby
CopyEdit
WPA handshake: C0:C1:C0:23:0F:A9
```

أي أنه تم التقاط Handshake بنجاح — وهو الملف الذي يحتوي على معلومات المصادقة.

ثالثاً: إجبار المستخدم على إعادة الاتصال:(Deauthentication)

```
bash
CopyEdit
aireplay-ng -0 10 -a C0:C1:C0:23:0F:A9 -c 86:40:A4:98:3D:BC
wlan0
```

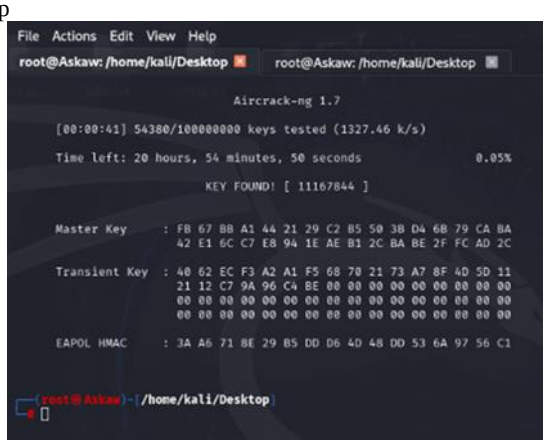
الشكل رقم(4): Deauthentication

الهجوم نفّذ 10 حزم DeAuth على المستخدم المرتبط.

تم تأكيد ACKs مما يعني أن الهجوم نجح في إجبار الجهاز على قطع الاتصال وإعادة المصادقة، وبالتالي تسريع التقاط الـhandshake

رابعاً: كسر كلمة المرور: تم استخدام ملف كلمات مرور password.txt في الهجوم:

```
bash
Copyedit
aircrack-ng -w password.txt -b C0:C1:C0:23:0F:A9 attackmoussa-
01.cap
```



الشكل رقم(5): كسر كلمة المرور

تم تجربة 54,380 كلمة مرور خلال أقل من دقيقة.

تم العثور على الكلمة الصحيحة:

```
CSS
Copyedit
KEY FOUND! [ 11167844]
```

جدول رقم (3) يوضح الملخص الفني:

العنصر	القيمة
عدد الحزم الملتقطة	30,906
نوع المصادقة	WPA2-PSK
تم العثور علىPMKID ؟	✅
تم تنفيذDeAuth ؟	✅ بنجاح مع ACK مرتفع
تم التقاطHandshake ؟	✅ من ملفpassword.txt

جدول رقم(4) يوضح تفاصيل الشبكة المستهدفة:(Askaw)

الخاصية	القيمة
BSSID	C0:C1:C0:23:0F:A9
ESSID	Askaw
التشفير	WPA2
نوع التشفير	CCMP
التوثيق	PSK
القناة	11
قوة الإشارة	-41
عدد الإطارات	2991
الأجهزة المتصلة	86:40:A4:98:3D:BC, 12:BE:F3:...

كما تم إرسال رسائل تصيد وهمية عبر مجموعات الواتساب باستخدام Social Engineering Toolkit لمحاكاة هجمات الهندسة الاجتماعية (Hadnagy, 2018).

السيناريو الثاني: اختبار اختراق الأجهزة

اختبار اختراق الأجهزة باستخدام أدوات الهندسة الاجتماعية Social Engineer Toolkit (SET)

الأدوات :

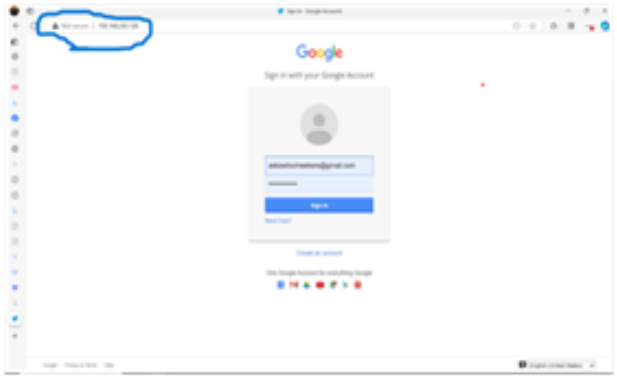
Gophish:لاختبارات التصيد الاحترافية

King Phisher:هجمات متقدمة بواجهة رسومية

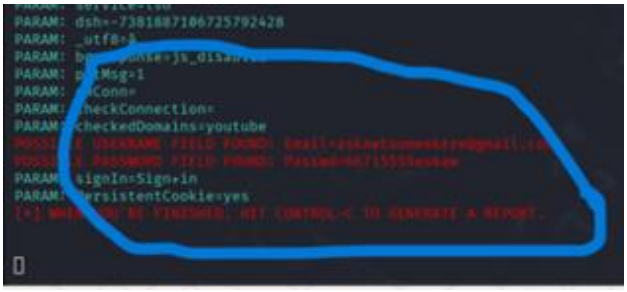
Evilginx2:لاختراق المصادقة الثنائية

تمت إجراء خمسة محاولات لعدد احتياله لاكتشاف حسابات المستخدمين عبر إرسال رابط وإظهار واجهة لموقع الهوتميل أو الجيميل لان اغلب المستخدمين يستخدمون هذا البريد الالكتروني و بإغوائه بأمور تهمه تظهر واجهة لإدخال الحساب وكلمة المرور ومن خلالها يتم معرفة حسابه كما هو موضح بالشكل التالي رقم (6).

تم إرسال رابط في مجموعة الواتساب وبعد النقر عليه ظهرت تأكيد بنافذة بريد الكتروني إلا أن الضحية لم يدرك عنوان الصفحة مزيفة وقام بإدخال بيانات البريد الالكتروني لجيميل Gmail وهي عملية احتيالية لمعرفة الحساب وهذه طريقة بسيطة يغفل عنها الكثيرون بسبب الطمع لحصول على شي بصورة سهلة وقد ناقش هذا الجانب الشريف(2020) مخاطر الثغرات الأمنية في التعليم العالي، مسلطاً الضوء على أهمية التهيئة السلوكية والمؤسسية ضمن سياسات الحماية. (الشريف، 2020).



الشكل رقم(6): يوضح تسجيل الدخول المزيف من خلال URL



الشكل رقم (7): يوضح على بيانات بريد الضحية

من الشكل رقم (7) نجد أن الpassword,الEmailقد تم الحصول عليهم من الصفحة جوجل المزيفة. حيث تمت التجربة بعدة طرق وذلك باستنساخ مواقع بعد معرفة بعض المعلومات عن الضحية وباستخدام الأداء يسهل الحصول على حساب الضحية بسهولة كما لا يمكن أن تعمل مع المواقع التي تستخدم CAPTCHA المصادقة الثنائية وتبين أكثر النماذج نجاحا كانت المبنية على تقنية cloner حيث حققت معدل نجاح بنسبة 85% في وقت وجيز بينما كان معدل النجاح في النماذج اليدوية custom اقل بكثير كما هو موضح في جدول رقم (5).

جدول رقم (5) يوضح التقنيات

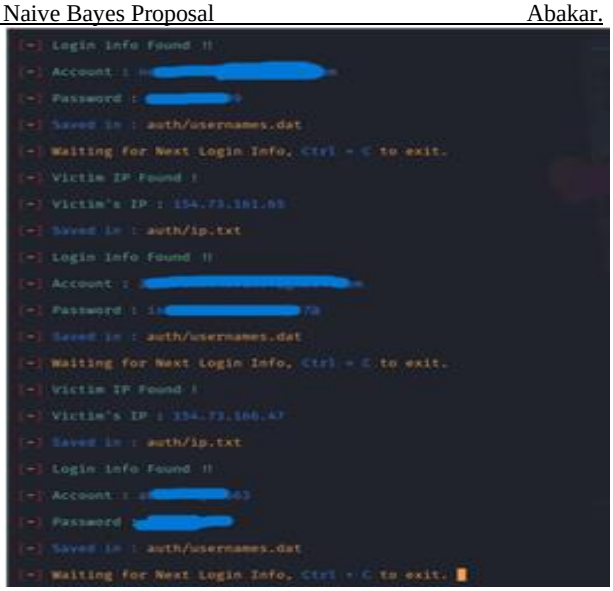
الطريقة	معدل النجاح	الوقت	الصعوبة
Templates	65%	2دقائق	منخفضة
Cloner	85%	5دقائق	متوسطة
Custom	45%	15+دقيقة	عالية

السيناريو الثالث: تحليل الثغرات الأمنية

حيث تمت هذه التجربة بغرض التأكد هل تم استيعاب التوعية من عدم النقر في أي رابط مجهول المصدر وكانت النتائج حسب التجربة باستخدام أداة Zphisher v2.3.5 تعمل في نظام تشغيل كالي لينكس وطريقة الهجوم باستخدام رابط وهمي باستخدام Cloudflare والهدف معرفة كلمة المستخدم وكلمة السر عبر واجهة وهمية مستخدما Snapchad. ضمن التطبيقات الموجودة وفيها العديد من التطبيقات يتم اختيار تطبيق معين حسب ميول الضحايا وهي طريقة سهلة تبدأ بتشغيل أداة Zphisher ثم اختيار الموقع المستهدف وإرسال الرابط عبر كتابة كلمات مثيرة للتضحية تجعله يضغط على الرابط ومنها يتم كشف تفاصيل بياناته كما هو موضح في الشكل أدناه

الشكل رقم(8): يوضح انتظار الضحية لينقر على الرابط

بالرغم من التوعية التي أجريت قبل تطبيق الاختبار لأعضاء هيئة التدريس والطلاب بعدم النقر أو الضغط لأي رابط مجهولة الهوية. إلا ان عملية التوعية غير كافية لحماية الأجهزة والشبكات من خلال التطبيق الفعلي وهو إرسال روابط وهمية في مجموعة الطلاب وأعضاء هيئة التدريس بكلية العلوم وتقنية الهندسية بجامعة الملك فيصل بتشاد، فأكدت الدراسة أن نسبة 51% كانوا ضحية للاحتيال كما هو موضح جزء من الجانب العملي في الشكل رقم (9).



شكل رقم(9): يوضح سرقة بيانات الضحية

تجربة استخدام خوارزمية Naïve Bayes في تحليل الرسائل من خلال التجارب السابقة لاحظ الباحث عدم استجابة أعضاء هيئة التدريس والطلاب لعملية التوعية بخطورة التعامل مع الروابط مجهولة المصدر والمقصود بهذه العبارة من خلال عنوان المصدر URL: http أو عدم معرفتهم بها ولذا تم اقتراح الاعتماد على خوارزمية ذكية تقوم بهذه العملية نيابة عنهم(An et al, 2025)، وتم اختيار خوارزمية Naive Bayes لسرعتها في كشف الهجمات السيبرانية ودقتها وسهل الفهم للمتدربين حيث تقوم هذه الخوارزمية بتصنيف وتحليل الرسائل على تطبيقات مثل واتساب والبريد الالكتروني بناء على خصائصها، وجود روابط خبيثة او مشبوهة، كلمات عاجلة (مثل الان، مهم، فوري)، وقد أظهرت الخوارزمية دقة جيدة في التنبؤ بالرسائل الاحتيالية. (عبدالله، 2022)

كدراسة مستقبلية تقوم بالأعمال البشرية نسبة لقلة الكوادر المتخصصة في هذا المجال ، وتشير هذه النتائج إلي أهمية دمج الخوارزمية الذكية في الأنظمة البريدية والأنظمة الداخلية بالجامعة لتحليل المحتوى والروابط قبل عرضها للمستخدم النهائي.(Verma وآخرون, 2023)، وتم تنفيذ جميع هذه الاختبارات مع الالتزام الكامل بالإطار الأخلاقي والقانوني للاختبارات الأمنية.

5. النتائج والتحليل

1.5. النتائج:

تم استخلاص النتائج الرئيسية للدراسة من خلال جمع البيانات عبر تنفيذ ثلاثة سيناريوهات ميدانية، والتي شملت:

أولاً: سيناريو اختبار اختراق الشبكة اللاسلكية

- تقييم مستوى تأمين البنية التحتية للشبكات
- قياس قوة أنظمة التشفير والمصادقة المعتمدة

ثانياً: سيناريو اختبار الوعي الأمني للمستخدمين

- تقييم استجابة مختلف الفئات لهجمات التصيد الاحتيالي.
- قياس مستوى القدرة على تمييز التهديدات الإلكترونية.

ثالثاً: سيناريو تحليل الثغرات الأمنية الشاملة.

- تقييم مستوى الحماية في الأجهزة والأنظمة.
- تحليل نقاط الضعف في السياسات الأمنية المعتمدة.

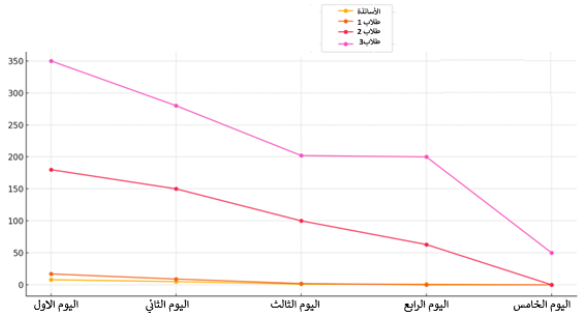
وقد تم توثيق نتائج هذه الاختبارات على مدى خمسة أيام متتالية في الجدول رقم (1)، الذي يوضح نسب نجاح محاولات الاختراق حسب كل فئة من فئات الدراسة، مما يوفر قاعدة بيانات غنية لتحليل مدى فعالية الإجراءات الأمنية الحالية وتحديد نقاط الضعف التي تحتاج إلى تعزيز.

تمثل هذه البيانات المجمعة أساساً لإجراء التحليلات الإحصائية اللاحقة واستخلاص التوصيات العملية لتعزيز أمن المعلومات في المؤسسات التعليمية.

جدول رقم(1) يوضح عدد نجاح اختبارات الاختراق حسب الفئة

الفئة	كمية العينة	عدد الاختراقات باليوم					المجموع	نسبة النجاح
		1	2	3	4	**5**		
الأساتذة	20	8	5	1	1	0	15	%15
طلاب 1	35	17	9	2	0	0	28	%16
طلاب2	186	180	150	100	63	0	493	%53
طلاب3	393	350	280	202	200	50	1082	%55
(طلاب وأساتذة)	634	555	444	305	264	50	1618	**%51**
راوتر	1	0	1	1	1	0	3	%60

يوضح الشكل رقم(1) التوزيع الزمني لاختبارات الاختراق على مدار خمسة أيام، حيث لوحظ أن طلاب التخصصات الأدبية(طلاب3) والعلمية (طلاب2) سجلوا اعلي معدلات النجاح في اليوم الأول، بينما أظهرت فئة الأساتذة وطلاب هندسة الحاسوب (طلاب1) وعياً امنياً ساهم في تقليل نسبة الاختراق.



الشكل رقم (1): يوضح عدد النجاحات في اختبارات الاختراق خلال خمسة أيام

2.5. التحليل الإحصائي للتجارب التطبيقية

توصيف البيانات:

شملت التجربة أربع فئات من الأجهزة المستخدمة من قبل :أساتذة(20)، طلاب1(35)، طلاب2(186)، طلاب3(393)، على مدى خمسة أيام . ولتفادي انحياز الحجم غير المتكافئ بين الفئات، تمّ اعتماد النِّسَب المئوية للاختراق كوحدة قياس موحّدة كما هو موضح في الجدول رقم(2)، قبل إجراء الاختبارات الاستدلالية. هذا الإجراء ينسجم مع الممارسات التحليلية المعاصرة التي تؤكد ضبط فروض الاختبارات عند وجود تفاوتات حجمية ملحوظة بين المجموعات (Field, 2013; Howell,2012)، تدعم أدبيات الحقل أن البيئات الجامعية تعاني ضغطًا متزايدًا من التصيد والهندسة الاجتماعية والتهديدات المتقدّمة، ما يبرّر اختيار مقاييس حسّاسة للفروق السلوكية بين الفئات (مثل الطلاب مقابل الأساتذة) عند تقييم المخاطر السيبرانية. وتشير تقارير حديثة إلى تصاعد دور العنصر البشري في الاختراقات، وارتفاع أحمال فرق الأمن في الجامعات نتيجة نقص الكفاءات والموارد المتخصصة. (العتيبي،2022؛ Hadngay,2018).

جدول رقم(2): يوضح نسبة الاختراق للفئات

اليوم	الأساتذة	طلاب1	طلاب2	طلاب3	الشبكة
1	%40	%49	%97	%89	%0
2	%25	%26	%80	%71	%100
3	%5	%6	%54	%51	%100
4	%5	%0	%19	%51	%100
5	%0	%0	%0	%13	%0

نتائجANOVA

تم إجراء تحليل التباين الأحادي (One-Way ANOVA) بين الفئات الأربع للأجهزة . حيث أظهر النتائج أن الفروق لم تصل إلى مستوى الدلالة الإحصائيـة عنـد $\alpha = 0.05$ ، مما يعني أن هناك تشابهًا كافيًا بين متوسطات الفئات على الأقل في بعض المقارنات، ولم يكن الاختلاف العام بين جميع الفئات واضحًا.

نتائج الاختبارات البَعدية(Welch's T-test)

جدول رقم (3): مقارنة بين الفئات الأربع

المقارنة	t	p-value	الاستنتاج
أساتذة و طلاب1	-0.0988	0.923849	غير معنوي
أساتذة و طلاب2	-1.7796	0.131366	غير معنوي
أساتذة و طلاب3	-2.7098	0.03225	فرق معنوي
طلاب1 و طلاب2	-1.6506	0.149629	غير معنوي
طلاب1 و طلاب3	-2.4518	0.042118	فرق معنوي
طلاب2 و طلاب3	-0.2259	0.827567	غير معنوي

حيث أظهرت المقارنات الزوجية في الجدول رقم(3) أن:

- فئة طلاب التخصصات الأدبية (طلاب3) يختلفون بشكل معنوي عن الأساتذة ($p = 0.032$) وطلاب هندسة الحاسوب(طلاب1) ($p =0 .042$) .
- لم تُسجّل فروق معنوية بين الأزواج الأخرى($p >0.05$) ، من ضمنها طلاب التخصصات العلمية مقابل طلاب التخصصات الأدبية ($P=0.828$) .هذه الفروق المحددة تدعم أن الفئة الأكثر ضعفًا هي فئة الطلاب التخصصات الأدبية،.(Armas, 2025) .

نتائج اختبار كاي تربيع(Chi-Square Test of Independence) :

تم استخدام هذا الاختبار بوصفه الإجراء الإحصائي الأنسب لفحص العلاقة بين الفئة الأكاديمية واحتمالية تعرّض الأجهزة للاختراق. ويعود اختيار هذا الاختبار إلى طبيعة البيانات محل الدراسة، حيث إن كلا المتغيرين فئويان (الفئة الأكاديمية: أساتذة، طلاب هندسة الحاسوب، طلاب التخصصات العلمية، طلاب التخصصات الأدبية؛ حالة الجهاز: مخترق/غير مخترق). بينما تعالج اختبارات مثل ANOVAو T-testالفروق في المتوسطات للمتغيرات الكمية، فإنها لا توفر دليلاً مباشرًا على وجود ارتباط بين المتغيرات الفئوية. ومن هنا جاء توظيف كاي تربيع للتحقق مما إذا كانت نسب الاختراق تختلف باختلاف الفئة الأكاديمية، أي لفحص استقلالية أو ترابط المتغيرين. وقد أسهم هذا الاختبار في تقديم دليل تكميلي يدعم نتائج ANOVAوT-test، حيث أكد أن الفروق المسجّلة بين المجموعات ليست عشوائية، بل مرتبطة ارتباطًا ذا دلالة إحصائية بمستوى الانتماء الأكاديمي(Agresti, 2019; Mchugh,2013; Scharp, 2015; Kim,2017; Field, 2020)

للتحقق من العلاقة بين الفئة الأكاديمية (أساتذة، طلاب1، طلاب2، طلاب3) (وحالة الجهاز) (مخترق / غير مخترق)، أُجري اختبار كاي تربيع على بيانات الأجهزة .($N = 634$) وكانت النتيجة = χ^2 ($3, N = 634$) : $25.34, p < 0.001$، ما يدل على وجود علاقة إحصائية قوية بين نوع الفئة واحتمالية الاختراق .هذه النتيجة تعكس أن اختلاف مستوى التعرض للاختراق بين الفئات ليس عشوائيًا، بل متأثرًا بعوامل مرتبطة بالفئة الأكاديمية والسياسات الأمنية الفردية والجماعية.

تحليل (الشبكة) الراوتر:

أظهرت بيانات (الشبكة) جهاز واحد معدل اختراق بلغ 60% (ثلاثة أيام من أصل خمسة) .

ونظرًا لكون المقام جهازًا واحدًا فقط، لم يُدرج في تحليلANOVA ، بل عولج وصفيًا باعتباره مؤشرًا على ضعف البنية التحتية . وهذا يتسق مع دراسات حديثة أبرزت أن البنية التحتية للشبكات تمثل نقطة ضعف رئيسية أمام الهجمات السيبرانية(Anderson, 2020 ؛ Zaid & others, 2024).

6. الاستنتاج العام والتوصيات:

1.6. الاستنتاج العام:

تكشف نتائج هذه الدراسة أن المؤسسات التعليمية – ومن ضمنها جامعة الملك فيصل في تشاد – تواجه ثغرات أمنية حرجة تتوزع بين البعد البشري والبعد التقني. فقد أظهرت التجارب أن ما نسبته 51% من المستخدمين وقعوا ضحية لمحاولات التصيد، وهو مؤشر واضح على هشاشة الثقافة الأمنية لدى شريحة واسعة من الطلاب، لاسيما عند مقارنتهم بالأساتذة الذين أبدوا مقاومة أعلى بكثير لهذه الهجمات.

وتتسق هذه النتيجة مع ما ذهب إليه (البكري، 2023 ; العتيبي، 2022 ; Hadnagy,2018) بشأن كون العامل البشري الحلقة الأضعف في منظومات الحماية، حيث يتجاهل الأفراد التحذيرات الأمنية بدافع الفضول أو الثقة المفرطة . كما أن نتائج التحليل الإحصائي (ANOVA وT-test) التي أبرزت فروقًا ذات دلالة إحصائية بين الفئات، تدعم ما توصلت إليه دراسات سابقة (Zhang & Others, 2022 ؛Alenezi, 2021) من أن التباين في مستويات الوعي الأمني يسهم مباشرة في تفاوت احتمالية التعرض للهجمات.

وعلى المستوى التقني، أظهرت اختبارات الاختراق للشبكات اللاسلكية أن الاعتماد على الإعدادات الافتراضية لأجهزة التوجيه (Routers) يمثل نقطة ضعف بالغة الخطورة، إذ أمكن كسر كلمات المرور خلال دقائق باستخدام أدوات مفتوحة المصدر. وتنسجم هذه النتيجة مع ما أشار إليه النوري (2022) من خطورة الاعتماد على إعدادات أمنية ضعيفة في شبكات الجامعات، وما قد يترتب عليها من سهولة الاستهداف والاختراق. كما أكد عطيف (2023) أن القيادات التعليمية ما زالت تعاني من قصور في الوعي السيبراني، الامر الذي يزيد من صعوبة تنفيذ استراتيجيات التحول الرقمي ويجعل السياسات الامنية اقل فاعلية. ومن ثم فان اجتماع هذه الثغرات التقنية مع ضعف الوعي المؤسسي يعزز هشاشة البنية الرقمية للجامعات، ويجعلها اكثر عرضة للهجمات الالكترونية المتكررة.

من جهة أخرى، تطرح الدراسة خيارًا مستقبليًا يتمثل في الاستفادة من الخوارزميات الذكية، وعلى رأسها Naive Bayes، لتعزيز قدرات الكشف المبكر عن التهديدات الإلكترونية. ورغم أن هذا النموذج لم يُختبر فعليًا ضمن نطاق هذه الدراسة، إلا أن بحوثًا سابقة (Saxe & Berlin, 2015؛ Salloum & others, 2021) أثبتت فعاليته العالية في تصنيف الرسائل والروابط المشبوهة بدقة تجاوزت 85%، مما يجعله توجهًا واعدًا لتطوير

حلول مؤسسية أكثر استدامة في المستقبل. كما أوضح الخطيب (2021) أن تقنيات الذكاء الاصطناعي تُمكّن المؤسسات من بناء أنظمة رصد أكثر قوة ضد الهجمات السيبرانية. وكذلك يؤكد الكوار (2023) أن الذكاء الاصطناعي أصبح محورًا رئيسيًا في مواجهة التهديدات السيبرانية المعاصرة.

القيود:

رغم القيمة التطبيقية التي تقدمها هذه الدراسة، إلا أنها تعاني من بعض القيود التي ينبغي أخذها في الاعتبار:

اقتصرت التجربة على جامعة واحدة، الأمر الذي يحد من إمكانية تعميم النتائج على بقية المؤسسات التعليمية.

لم يتم تطبيق خوارزمية Naive Bayes فعليًا على بيانات الدراسة، واقتصر طرحها كمقترح بحثي مستقبلي.

جُمعت البيانات خلال فترة زمنية قصيرة (خمسة أيام)، وهو ما قد لا يعكس جميع أنماط السلوك الأمني لدى المستخدمين.

الأهمية:

تتمثل القيمة المضافة لهذه الدراسة في إبرازها أن أي استراتيجية فعالة لتعزيز الأمن السيبراني في الجامعات ينبغي أن تقوم على مقاربة مزدوجة:

- تقنية: عبر تحصين البنية التحتية للشبكات والتخلص من نقاط الضعف في الإعدادات.
- سلوكية: عبر رفع مستوى وعي المستخدمين وتدريبهم بشكل مستمر على مواجهة التهديدات الإلكترونية.

2.6. التوصيات:

بناء على نتائج التحليل والملاحظات المستخلصة من التجارب التطبيقية، تقدم الدراسة التوصيات التالية لتعزيز أمن المعلومات وحماية الشبكات والأجهزة داخل المؤسسات التعليمية، وخاصة في البيئات المشابهة لجامعة الملك فيصل بتشاد:

- ✓ تعزيز مكانة المعلومات كمورد استراتيجي للمؤسسة: يجب أن تُعامل البيانات والمعلومات باعتبارها أحد الأصول الحيوية التي تُمثل الأساس في صناعة القرار وتطوير الأداء المؤسسي، الأمر الذي يتطلب إدراج أمن المعلومات ضمن أولويات الإدارة العليا وتخصيص الموارد الكافية لحمايته. وإدراج اختبار توعوي دوري ضمن المناهج الجامعية لقياس مدى وعي الطلبة بالهندسة الاجتماعية.
- ✓ فرض استخدام البريد الجامعي الرسمي في جميع المعاملات الأكاديمية والإدارية للحد من استغلال البريد الشخصي في هجمات التصيد الإلكتروني.
- ✓ دمج تقنيات الذكاء الاصطناعي، وعلى رأسها خوارزمية Naive Bayes، لرصد التهديدات الأمنية بشكل آلي ومستمر
- ✓ على المؤسسات التعليمية تفعيل دورها في مواجهة التهديدات من خلال تعزيز البنية التحتية الرقمية، وتطوير برامج توعوية، واعتماد سياسات تنظيمية داعمة للأمن السيبراني. (بغدادي، شيماء السيد بغدادي 2024).

7. المراجع:

1.7. المراجع العربية:

البكري، ن .(2023). *فاعلية برامج التوعية الأمنية الإلكترونية في تقليل الهجمات السيبرانية* . المجلة السعودية لأمن المعلومات.

بغدادي، ش .س .(2024). *متطلبات تفعيل دور المؤسسات التعليمية في مواجهة حرب المعلومات .المجلة العربية للدراسات المستقبلية.*

الحسيني، أ .ع .(2022). *تحديات التحول الرقمي في التعليم بالجامعات المصرية ورؤى مستقبلية لتطوير سبل التعليم بها . المجلة العربية للعلوم التربوية والاجتماعية.*

الخطيب، ع .(2021). *أثر استخدام الذكاء الاصطناعي في تعزيز أمن المعلومات* .مجلة جامعة الأقصى للعلوم الإنسانية.

الجنفاوي، خ .(2021). *التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني* .المجلة العربية للآداب والدراسات الإنسانية.

حمدان، س .(2021). *وعي أفراد الأسرة بمفهوم الأمن السيبراني. المجلة العربية للعلوم الاجتماعية.*

الشريف، ه .(2020). *الثغرات السيبرانية المرتبطة بالأجهزة الذكية في بيئة التعليم العالي*. المجلة العربية لتقنية المعلومات.

العتيبي، ف .(2022). *أثر ضعف الوعي الأمني على اختراقات الحسابات الشخصية في الجامعات السعودية* .مجلة دراسات أمن المعلومات.

عبد الله، س .(2022). *دور خوارزمية التصنيف في كشف رسائل التصيد الإلكتروني* (رسالة ماجستير غير منشورة). جامعة الملك سعود.

الكوار، م .م .(2023). *الذكاء الاصطناعي وتطبيقاته المعاصرة*. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات.

النوري، أ .(2022). *تقييم كفاءة أدوات اختبار الاختراق مفتوحة المصدر : دراسة حالة كالي لينكس* . المؤتمر السعودي للأمن السيبراني، جامعة الملك فهد للبترول والمعادن.

عطيف، أ .(2023). *الوعي بالأمن السيبراني والتحول الرقمي لدى القيادات التعليمية* . مجلة جامعة جازان للعلوم الإنسانية،25 -115 ,(2) 138.

زيد، ت.، وآخرون .(2024). *الاتجاهات الناشئة في الأمن السيبراني* :رؤية شاملة .المجلة الدولية للأمن السيبراني وتكنولوجيا المعلومات،12 (3), 45-67.

2.7. المراجع الأجنبية

Agresti, A. (2019). *An introduction to categorical data analysis* (3rd ed.). Wiley.

Alenezi, M. (2021). *Deep Dive into Digital Transformation in Higher Education Institutions*, Education Sciences, 11(12), 770. https://doi.org/10.3390/educsci11120770

Anderson, R.(2020). Security engineering; A guide to building dependable distributed system(3rd ed.). Wiley

An, P., Shafi, R., Mughogho, T., & Onyango, O. A. (2025). *Multilingual Email Phishing Attacks Detection using OSINT and Machine Learning (1 إصدار)*. arXiv. https://doi.org/10.48550/ARXIV.2501.08723

Field, A. (2020). *Discovering statistics using IBM SPSS statistics* (5th ed.). Sage

Kim, H. Y. (2017). Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. *Restorative Dentistry & Endodontics, 42*(2), 152–155. https://doi.org/10.5395/rde.2017.42.2.152

Marks, A. & others (2020*), Digital Transformation in Higher Education: A Framework for Maturity Assessment. International Journal of Advanced Computer Science and Applications 11(12)*

Verma, S., Ayala-Rivera, V., & Portillo-Dominguez, A. O. (2023*). Detection of Phishing in Mobile Instant Messaging Using Natural Language Processing and Machine Learning*. 2023 11th International Conference in Software Engineering Research and Innovation (CONISOFT), 159–168. https://doi.org/10.1109/*CONISOFT58849.2023.00029*

Zhang, Z., & Hamadi, H. A. Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence in Cyber Security: *State-of-the-Art in Research. IEEE Access, 10, 93104–93139.*

https://doi.org/10.1109/ACCESS.2022.3204051.

McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, *23*(2), 143–149. https://doi.org/10.11613/BM.2013.018

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking. Wiley*.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. Procedia Computer Science, 189, 19–28. https://doi.org/10.1016/j.procs.2021.05.077

Saxe, J., & Berlin, H. (2015). *Malware Data Science*: Attack detection and attribution. No Starch Press

Sharpe, D. (2015). Chi-square test is statistically significant: Now what? *Practical Assessment, Research, and Evaluation*, *20*(8), 1–10. https://doi.org/10.7275/tbfa-x148