



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف - المسيلة



الرقم التسلسلي:...../.....

رقم التسجيل : ط1- 35088052

رقم التسجيل : ط2 - 35078875

**مستوى الوعي بالأمن السيبراني لدى طلبة الاعلام الآلي
بجامعة محمد بوضياف المسيلة
دراسة ميدانية على طلبة الماستر 1 بكلية الاعلام الآلي**

مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والاتصال

تخصص : اتصال وعلاقات عامة

إشراف الأستاذة:

د/ فقيري ليلي

إعداد الطالبتين:

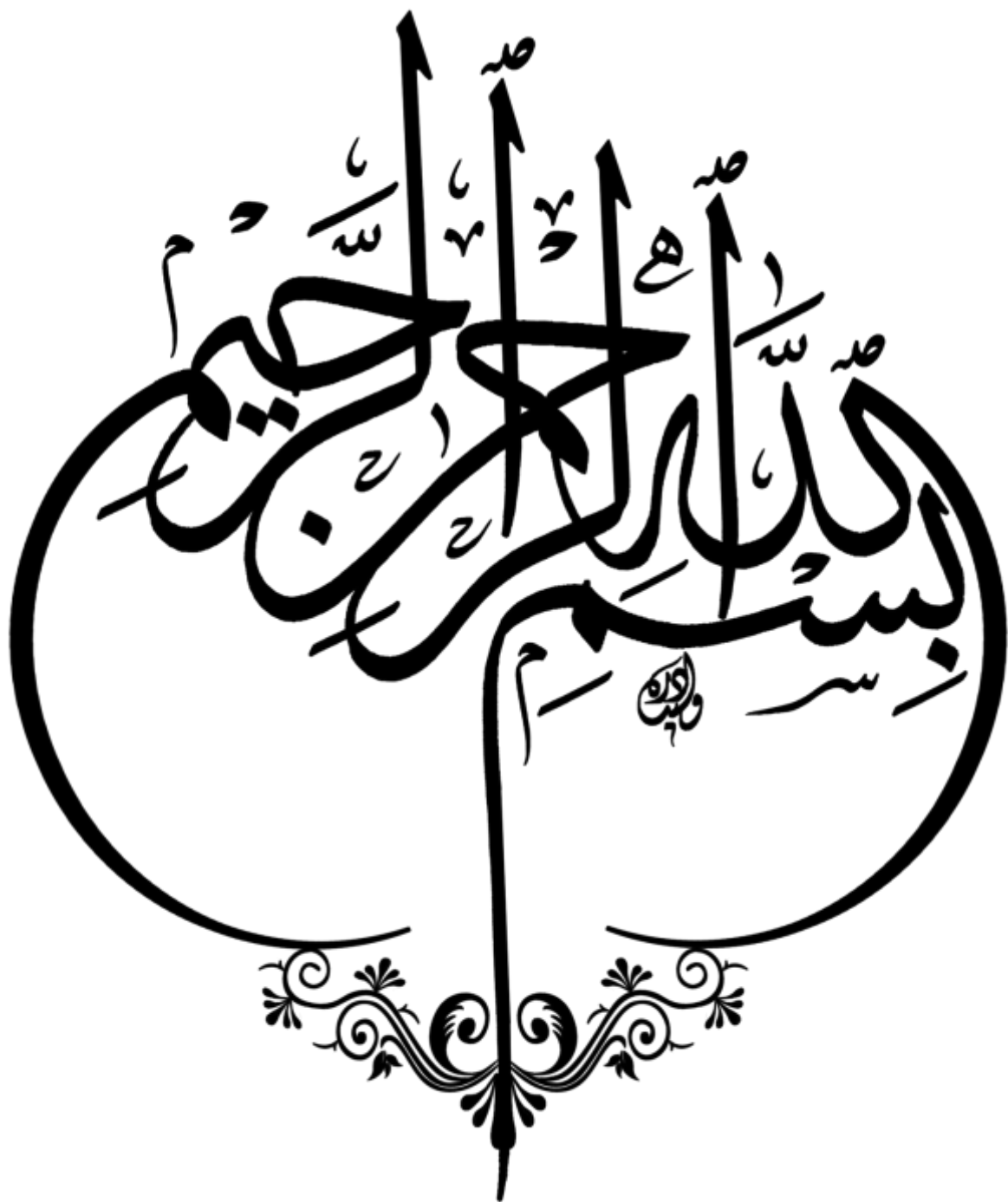
■ بشيري شيماء

■ ولهة مروة

أمام لجنة المناقشة المكونة من السادة:

الاسم واللقب	الرتبة العلمية	الصفة
د. جلول بوربابة	أستاذ محاضر-أ-	رئيسا
د. ليلي فقيري	أستاذ محاضر-أ-	مشرفا
د. الشيخ بن عيسى	أستاذ محاضر-أ-	ممتحنا

السنة الجامعية: 2025-2026





الجامعة الجزائرية الديمقراطية الشعبية
الجامعة محمد بوضياف - المسيلة
FACULTY OF HUMANITIES
AND SOCIAL SCIENCES

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
جامعة محمد بوضياف بالمسيلة
University Mohamed Boudiaf of M'sila



جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Faculty of Humanities and Social Sciences
Vice-Deanship of the College for Studies and
Student Issues

كلية العلوم الإنسانية والاجتماعية
تأية العمادة للدراسات والمسابيل المرتبطة بالطلبة
الرقم: 2026/

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي (ة) أدناه :

السيد(ة): **بنتي شيماء**

الصفة (طالب, أستاذ باحث, باحث دائم): **طالبة**

الحامل لبطاقة التعريف الوطنية رقم: **110031038003360005**

الصادرة بتاريخ: **23.07.03** عن دائرة: **امجد**

المسجل (ة) بكلية: **العلوم الإنسانية والاجتماعية قسم: علوم الإعلام والاتصال**

تخصص: **اتصال وعلاقات عامة** تحت رقم التسجيل: **35088052**

والمكلف بإنجاز أعمال بحث (مذكرة التخرج, مذكرة ماستر, مذكرة ماجستير, أطروحة دكتوراه)

عنوانها: **مستوى الوعي بالآمن للأهم السبراني لدى طلبة**

الإعلام الإلكتروني بجامعة محمد بوضياف بالمسيلة

دراسة ميدانية على طلبة الكلية كمتأثرين بكلية علوم الإعلام والاتصال

أصرح بشرفي بأنني التزم بالمعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه

المسيلة في: **07.06.2026**

إمضاء المعني (ة):



المرجع: القرار الوزاري رقم: 933 المؤرخ في: 28-07-2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها.



الكلية الإنسانية والاجتماعية
FACULTY OF HUMANITIES
AND SOCIAL SCIENCES

الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة محمد بوضياف بالمسيلة

University Mohamed Boudiaf of M'sila

Faculty of Humanities and Social Sciences

Vice-Deanship of the College for Studies and

Student Affairs



جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية العلوم الإنسانية والاجتماعية
نيابة العادة للدراسات والمسائل المرتبطة بالطلبة
الرقم: 2026/

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

انا الممضي (ة) ادناه :

السيد(ة): ولاحد حروية

الصفة(طالب, استاذ باحث, باحث دائم): طالبة

الحامل لبطاقة التعريف الوطنية رقم: 11 00 20 99 50 34 26 00 04

الصادرة بتاريخ: 13-04-2026 عن دائرة: المسيلة

المسجل(ة) بكلية: علوم الإنسان والعلوم الاجتماعية قسم: العلوم والانتماء

تخصص: انتماء ومسائل عامة تحت رقم التسجيل: 35 78 8 75

والمكلف بإنجاز أعمال بحث(مذكرة التخرج, مذكرة ماستر, مذكرة ماجستير, أطروحة دكتوراه).

عنوانها: مسألة الوعي بالانتماء اليك لدى طلبة العلوم الاجتماعية

جامعة محمد بوضياف بالمسيلة

دراسة علمية حول طلبة الماجستير بكلية الرياضيات والعلوم الاجتماعية

اصرح بشرفي بالني التزم بالمعايير العلمية والمنهجية ومعايير الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور اعلاه

المسيلة في: 2026-06-07

امضاء المعنى (ة):

18



المرجع: القرار الوزاري رقم: 933 المؤرخ في: 2016-07-28 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها.

عن رئيس المجلس العلمي العالي
وبتوقيع: م. بوزياف
بمساعدة: م. بوزياف



كلية العلوم
الإنسانية والاجتماعية
FACULTY OF HUMANITIES
AND SOCIAL SCIENCES

الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة محمد بوضياف بالمسيلة

University Mohamed Boudiaf of M'sila



جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Faculty of Humanities and Social Sciences

Vice-Deanship of the College for Studies and

Student Affairs

كلية العلوم الإنسانية والاجتماعية
نيابة العمادة للدراسات والمسائل المرتبطة بالطلبة

وثيقة ايداع مذكرة ماستر

الموضوع: **مشروع الوعي بالاحصاء البيروني لدى طلبة الإعلام الخليل بجامعة ماسيلة**
بوضياف المسيلة دراسة ميدانية على طلبة الحامر 1 بكلية الرياضيات
والاعلام الخليل

إعداد الطلبة:

1- **يتوب بيجاد** رقم التسجيل: **35 880 52**
2- **ولعة خروقة** رقم التسجيل: **35 788 75**
القسم: **اعلام واتصال** التخصص: **اتصال وعلامة تجارية**
إشراف: **د. افقيروا ليلي** الرتبة:

أقر بأنني تابعت العمل المذكور أعلاه في جلسات إشرافية طويلة الموسم الجامعي: 2024-2025 وأسمح بإيداعه على مستوى ادارة القسم للمناقشة والتقييم.

رئيس فريق الاختصاص:

موافقة وإمضاء الاستاذ(ة) المشرف(ة):

رئيس القسم:



شكر و عرفان

قال رسولنا عليه أفضل الصلاة وأزكى التسليم: (من لم يشكر الناس
لم يشكر الله)
نحمد الله على توفيقه لنا دائما لإتمام هذا العمل، فلولا توفيقه لما
وصلنا إلى هنا
نتقدم بجزيل الشكر والتقدير إلى الأستاذ المشرف أ. د/ **فقيري**
ليلي على جهوده الجبارة وصبره الطويل معنا وعلى توجيهاته
ومعلوماته القيمة التي ساهمت في إثراء موضوع دراستنا فجزاء الله
عنا خير الجزاء
كما نتقدم بجزيل الشكر إلى اللجنة المناقشة على قبولهم مناقشة
مذكرتنا
كما نتقدم بالشكر لكل أساتذة قسم **الاعلام والاتصال**.
وإلى كل من ساهم معنا من قريب أو بعيد وقدم لنا يد العون في هذا
العمل



إهداء

إلى من كان دعاؤهم سندي،
و...ومن تعبوا بصمت ليصل حلمي إلى هذا اليوم
إلى أمي وأبي، أطل الله في عمرهما،
أنتم أجمل نعمة وأعظم فخر.

إلى كل من آمن بي حين تعبت،
ووقف معي في لحظات الضغط واليأس،
إلى من شاركني الطريق ولو بكلمة طيبة أو دعوة صادقة.

أهدي ثمرة جهدي وتخرجي هذا،
بعد سنوات من التعب والسهر والمحاولات،
فالحمد لله الذي بنعمته تتم الصالحات.



إهداء

نهدي هذا العمل:

-إلى من أوحانا بهما برا وإحسانا ،وسمرا على تعليمنا وحثنا
إلى الدراسة و أناروا لنا الطريق و ضحوا من أجلنا الوالدين
العزيزين.

* كما نهدي بحثنا إلى أفراد الأسرة الإخوة و الأخوات.

-من ساندنا في أفراحنا و أحزاننا الأصدقاء

-إليكم جميعا هذا البحث من بستان العلم.

هدفت هذه الدراسة إلى تسليط الضوء على مستوى "الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي بجامعة محمد بوضياف بالمسيلة" للكشف عن طبيعة إدراكهم للمخاطر الرقمية ومدى امتلاكهم للثقافة الوقائية اللازمة في التعامل مع التهديدات الإلكترونية المتزايدة. وقد أظهرت الدراسة أن الوعي بالأمن السيبراني يمثل ركيزة جوهرية لحماية الأصول المعلوماتية، حيث تبين أن التفاعل الرقمي المسؤول يتطلب تجاوز المعرفة النظرية كما أكدت النتائج على دور الوسط الجامعي في تعزيز هذه الثقافة لدى الطلبة باعتبارهم العنصر الأساسي في تأمين الشبكات والأنظمة مستقبلاً موصيةً بضرورة تكثيف البرامج التوعوية والتدريبات العملية لرفع كفاءة الطلبة في مواجهة التحديات الأمنية المعاصرة والحد من آثار الاختراقات الرقمية. **الكلمات المفتاحية:** الأمن السيبراني، الوعي الرقمي، التهديدات الإلكترونية، الوسط الجامعي، طلبة الإعلام الآلي.

Abstract :

This study aimed to highlight the level of "Cybersecurity Awareness among Computer Science students at Mohamed Boudiaf University of M'Sila", to assess their perception of digital risks and their ability to adopt effective preventive measures against increasing electronic threats. The study reveals that cybersecurity awareness is a fundamental pillar for protecting information assets, indicating that responsible digital interaction requires moving beyond theoretical knowledge

The results also emphasize the role of the university environment in fostering this culture among students, as they are the primary actors in securing networks and systems in the future. The study recommends intensifying awareness programs and practical training to enhance students' competency in facing contemporary security challenges and mitigating the impact of digital breaches.

Keywords: Cybersecurity, digital awareness, cyber threats, university environment, computer science students.

فهرس المحتويات

الفهرس	
الصفحة	العنوان
	شكر وعرفان
	إهداء
	ملخص
I	الفهرس
III	قائمة الجداول
VI	قائمة الأشكال
أ	مقدمة
الفصل الأول: الإطار المنهجي	
3	1) الإشكالية :
4	2) الأسئلة الفرعية :
4	3) أهمية الدراسة وأهدافها
5	4) أسباب اختيار الموضوع
6	5) منهج الدراسة وأدواتها :
7	6) مجتمع الدراسة والعينة:
7	7) خصائص مجتمع الدراسة:
8	8) حدود الدراسة:
9	9) مصطلحات الدراسة:
12	10) المقاربات النظرية للدراسة :
14	11) الدراسات السابقة
الفصل الثاني: الفضل النظري	
19	تمهيد
20	المبحث الأول: الأمن السيبراني وأبعاده النظرية
20	المطلب الأول: ماهية الأمن السيبراني (المفهوم، الشأة، الخصائص)
25	المطلب الثاني: عناصر الأمن السيبراني وأبرز تهديداته الرقمية
28	المطلب الثالث: أهمية وأهداف الأمن السيبراني وشروط تحقيقه
30	المطلب الرابع: النظريات المفسرة للأمن السيبراني

32	المبحث الثاني : الوعي بالأمن السيبراني في الوسط الجامعي
32	المطلب الأول : تعريف الوعي السيبراني
33	المطلب الثاني: أهمية الوعي بالأمن السيبراني في الجامعات
33	المطلب الثالث : دور الجامعات في تعزيز الوعي بالأمن السيبراني
34	المطلب الرابع: استراتيجيات تعزيز الوعي السيبراني في الوسط الجامعي
36	خلاصة
الفصل الثالث: الفصل التطبيقي	
38	تمهيد
39	عرض وتحليل النتائج
39	أ/ تحليل البيانات الوصفية:
43	ب/ تحليل أسئلة الاستبيان:
43	أولا/ الجداول البسيطة
43	المحور الأول: مستوى المعرفة بالأمن السيبراني
55	المحور الثاني: مصادر الوعي بالأمن السيبراني
67	المحور الثالث: الممارسات والسلوكيات الرقمية للطلبة
81	المحور الرابع: إدراك التهديدات السيبرانية وانعكاساتها
93	المحور الخامس: تقييم دور الجامعة وسبل التعزيز
105	ثانيا/ الجداول المركبة
113	الاستنتاج العام للدراسة
114	مناقشة النتائج على ضوء التساؤلات والدراسات السابقة
116	خاتمة
119	قائمة المصادر والمراجع
122	ملاحق

قائمة الجداول

الرقم	العنوان	الصفحة
1.	الجدول رقم (01) يوضح توزيع أفراد عينة الدراسة حسب متغير الجنس	39
2.	الجدول رقم (02) يوضح توزيع أفراد عينة الدراسة حسب متغير السن	40
3.	الجدول رقم (03) يوضح توزيع أفراد عينة الدراسة حسب متغير التخصص	41
4.	الجدول رقم (04) يوضح توزيع أفراد عينة الدراسة حسب متغير التعرض للاختراق	42
5.	الجدول رقم (05) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (01)	43
6.	الجدول رقم (06) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (02)	45
7.	الجدول رقم (07) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (03)	47
8.	الجدول رقم (08) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (05)	49
9.	الجدول رقم (09) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (06)	51
10.	الجدول رقم (10) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (07)	53
11.	الجدول رقم (11) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (08)	55
12.	الجدول رقم (12) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (09)	57
13.	الجدول رقم (13) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (10)	59
14.	الجدول رقم (14) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (11)	61
15.	الجدول رقم (15) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (12)	63
16.	الجدول رقم (16) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (13)	65
17.	الجدول رقم (17) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (14)	67
18.	الجدول رقم (18) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (15)	69
19.	الجدول رقم (19) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (16)	71
20.	الجدول رقم (20) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (17)	73
21.	الجدول رقم (21) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (18)	75
22.	الجدول رقم (22) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (19)	77
23.	الجدول رقم (23) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (20)	79
24.	الجدول رقم (24) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (21)	81
25.	الجدول رقم (25) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (22)	83
26.	الجدول رقم (26) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (23)	85
27.	الجدول رقم (27) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (24)	87

89	الجدول رقم (28) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (25)	28
91	الجدول رقم (29) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (26)	29
93	الجدول رقم (30) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (27)	30
95	الجدول رقم (31) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (28)	31
97	الجدول رقم (32) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (29)	32
99	الجدول رقم (33) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (30)	33
101	الجدول رقم (34) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (31)	34
103	الجدول رقم (35) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (32)	35
105	الجدول رقم (36) إجابات أفراد عينة الدراسة على البند رقم (1) حسب الجنس	36
106	الجدول رقم (37) إجابات أفراد عينة الدراسة على البند رقم (02) حسب الجنس	37
107	الجدول رقم (38) إجابات أفراد عينة الدراسة على البند رقم (05) حسب الجنس	38
108	الجدول رقم (39) إجابات أفراد عينة الدراسة على البند رقم (08) حسب الجنس	39
109	الجدول رقم (40) إجابات أفراد عينة الدراسة على البند رقم (13) حسب الجنس	40
109	الجدول رقم (41) إجابات أفراد عينة الدراسة على البند رقم (15) حسب الجنس	41
110	الجدول رقم (42) إجابات أفراد عينة الدراسة على البند رقم (18) حسب الجنس	42
111	الجدول رقم (43) إجابات أفراد عينة الدراسة على البند رقم (21) حسب الجنس	43
111	الجدول رقم (44) إجابات أفراد عينة الدراسة على البند رقم (25) حسب الجنس	44

قائمة الأشكال

الرقم	العنوان	الصفحة
1.	الشكل رقم (01) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير الجنس	39
2.	الشكل رقم (02) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير السن	40
3.	الشكل رقم (03) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير التخصص	41
4.	الشكل رقم (04) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير التعرض للاختراق	42
5.	الشكل رقم (05): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (01)	44
6.	الشكل رقم (60) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (02)	46
7.	الشكل رقم (07): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (03)	48
8.	الشكل رقم (08): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (05)	50
9.	الشكل رقم (09): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (06)	52
10.	الشكل رقم (10): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (07)	54
11.	الشكل رقم (11): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (08)	56
12.	الشكل رقم (12): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (09)	58
13.	الشكل رقم (13): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (10)	60
14.	الشكل رقم (14): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (11)	62
15.	الشكل رقم (15): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (12)	64
16.	الشكل رقم (16): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (13)	66
17.	الشكل رقم (17): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (14)	68
18.	الشكل رقم (18): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (15)	70
19.	الشكل رقم (19): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (16)	72
20.	الشكل رقم (20): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (17)	74
21.	الشكل رقم (21): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (18)	76
22.	الشكل رقم (22): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (19)	78
23.	الشكل رقم (23): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (20)	80
24.	الشكل رقم (24): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (21)	82
25.	الشكل رقم (25): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (22)	84

86	الشكل رقم (26): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (23)	26
88	الشكل رقم (27): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (24)	27
90	الشكل رقم (28): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (25)	28

مقدمة

مقدمة:

يشهد العالم المعاصر ثورة رقمية متسارعة أحدثتها التطورات في تكنولوجيا المعلومات والاتصال ،حيث أصبحت الوسائط الرقمية والأنظمة الإلكترونية ركيزة أساسية في الحياة اليومية وعنصر جوهري في أساليب العمل والتعلم والتفاعل داخل المجتمعات الحديثة.

وفي ظل هذا التحول الرقمي، أصبحت المؤسسات الجامعية والتعليمية في مقدمة الفضاءات التي تأثرت بهذه الطفرة التكنولوجية حيث تحول الاعتماد على هذا الفضاء الافتراضي واقعاً حتمياً لا غنى عنه في تبادل المعارف ورغم هذا التدفق الإعلامي والمعلوماتي الهائل قد أتاح فرصاً واسعة لتطوير البحث العلمي وتسهيل التواصل إلا أنه أفرز في المقابل بيئة معقدة واكبتها تهديدات سيبرانية وهجمات إلكترونية متطورة تتجاوز الحدود التقليدية مما جعل من حماية الأمن المعلوماتي تحدياً مستمراً يواجه الأنظمة والمستخدمين على حد سواء.

وهنا تبرز الحاجة إلى بناء ثقافة رقمية واعية لدى مستخدمي هذه الشبكات لمواجهة تلك التهديدات داخل المحيط الجامعي لم تعد تتوقف على جودة الأجهزة والبرامج المستعملة بقدر ما ترتبط بنوعية السلوك الاتصالي الذي يتبناه الأفراد ومدى قدرتهم على اتخاذ القرارات الصحيحة أثناء التعامل مع البيانات والمعارف المتداولة يومياً.

انطلاقاً من هذا سعيانا إلى دراسة واقع الوعي بالأمن السيبراني لدى طلبة الجامعة من خلال هيكلية هذا البحث في ثلاثة فصول متكاملة فقد خصصنا الفصل الأول الجانب النظري تحت عنوان "الأمن السيبراني وأبعاده النظرية" متناولين فيه ماهية الأمن السيبراني ونشأته، وعناصره وأبرز تهديداته إضافة إلى أهميته و أهدافه والنظريات المفسرة له.

أما الفصل الثاني، فقد حمل عنوان "الوعي بالأمن السيبراني في الوسط الجامعي" حيث ركزنا فيه على تحديد ماهية الوعي السيبراني وأهميته في الوسط الجامعي مع استعراض دور الجامعة في تعزيز هذا الوعي واستراتيجيات تحقيقه.

وأخيراً، جاء الفصل الثالث ليمثل الإطار التطبيقي للدراسة حيث عرضنا فيه نتائج الدراسة الميدانية وتحليلها وصولاً إلى استنتاجات وتوصيات عملية تخدم موضوع البحث.

الفصل الأول

- الإطلار المنهجي -

1) الإشكالية :

يمثل الأمن السيبراني حجر الزاوية في حماية أصول المعلومات والبيانات الحيوية في ظل التوسع المتسارع للمجتمعات حيث فرضت التكنولوجيا الحديثة نفسها بقوة على مختلف مجالات الحياة، وخاصة في المجال الإعلامي. فقد أصبحت وسائل الإعلام تعتمد بشكل متزايد على التقنيات الرقمية في إنتاج المحتوى ونشره والتفاعل مع الجمهور، الأمر الذي جعل من التحول الرقمي ضرورة حتمية وليس مجرد خيار، تفرضه متطلبات العصر والتطورات المتلاحقة في بيئة الاتصال.

وقد انعكس هذا التحول بشكل واضح على طبيعة الممارسة الإعلامية، خاصة في ظل بروز الإعلام الرقمي الذي يتميز بسرعة انتشار المعلومات، والتفاعلية العالية، وتعدد مصادر المحتوى، مما أفرز بيئة إعلامية جديدة تتسم بالانفتاح والتعقيد في آن واحد. وفي هذا السياق، بات من الضروري على الطلبة الجامعيين، لاسيما في التخصصات المرتبطة بالتكنولوجيا والإعلام، اكتساب مهارات رقمية متقدمة تمكنهم من التكيف مع هذه التحولات والمساهمة الفعالة في إنتاج محتوى إعلامي يتماشى مع متطلبات العصر الرقمي.

وتبرز أهمية هذا الموضوع في السياق الجزائري في ظل التوسع الكبير في استخدام الإنترنت، حيث تشير تقارير حديثة إلى ارتفاع نسبة مستخدمي الإنترنت في الجزائر، وهو ما يعكس حجم الانخراط الواسع في الفضاء الرقمي. كما تظهر المعطيات أن فئة الشباب تُعد من الفئات الأكثر نشاطاً في هذا المجال، خاصة مع انتشار وسائل التواصل الاجتماعي التي يستخدمها عدد كبير من الأفراد بشكل يومي. وفي المقابل، تعرف الجزائر تزايداً ملحوظاً في التهديدات السيبرانية، إذ يتم تسجيل عدد معتبر من محاولات التصيد الاحتيالي، وهو ما يعكس حجم المخاطر التي قد تهدد المستخدمين في البيئة الرقمية. كما أظهرت دراسات ميدانية على الطلبة الجامعيين أن مستوى الوعي بالأمن السيبراني يبقى متوسطاً، في حين أن نسبة معتبرة من الطلبة سبق لهم التعرض لجرائم إلكترونية دون التبليغ عنها.

وفي الإطار الجامعي الجزائري، يُعد طلبة الإعلام الآلي من الفئات التي تعتمد بشكل كبير على استخدام التكنولوجيا الرقمية، بحكم طبيعة تكوينهم الأكاديمي الذي يركز على البرمجة، وقواعد البيانات، وشبكات الاتصال، وأمن المعلومات.

كما أن ممارستهم اليومية تتمحور حول التعامل مع الأنظمة الرقمية والتطبيقات المختلفة، الأمر الذي يجعلهم في مواجهة مباشرة مع مختلف أشكال التهديدات السيبرانية، بل وأكثر عرضة لها مقارنة بغيرهم من الطلبة في ومن هذا المنطلق، تبرز إشكالية هذه الدراسة في محاولة الكشف عن مستوى وعي طلبة الإعلام الآلي بالأمن السيبراني، ومدى إدراكهم النظري والتطبيقي للمخاطر الرقمية، إلى جانب تحليل طبيعة سلوكياتهم وممارساتهم داخل

الفضاء الرقمي، ومدى التزامهم بإجراءات الحماية والأمن المعلوماتي. كما تسعى الدراسة إلى استكشاف دور التكوين الجامعي في تنمية هذا الوعي، ومدى مساهمته في ربط المعارف النظرية بالتطبيقات العملية في مجال الأمن السيبراني، خاصة في ظل الفجوة التي قد تظهر أحياناً بين ما يُدرس أكاديمياً وما يُمارس فعلياً .

وعليه ، تتمحور الإشكالية الرئيسية لهذه الدراسة حول السؤال التالي :

ما مستوى الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي بجامعة محمد بوضياف بالمسيلة؟

(2) الأسئلة الفرعية :

وللإجابة عن الاشكالية الرئيسية نطرح مجموعة من الأسئلة الفرعية، من بينها:

أ- ما مستوى معرفة طلبة الإعلام الآلي بمفاهيم ومخاطر الأمن السيبراني؟

ب - ما أهم مصادر اكتساب هذا الوعي؟

ت- ما طبيعة الممارسات والسلوكيات الرقمية التي يعتمد عليها الطلبة في استخدام الوسائط الرقمية؟

ج- كيف يدرك الطلبة التهديدات السيبرانية وانعكاساتها على حياتهم الأكاديمية والاجتماعية؟

ح- ما تقييم الطلبة لدور الجامعة في تعزيز هذا الوعي؟

(3) أهمية الدراسة وأهدافها

(أ) الأهمية :

تكتسب هذه الدراسة أهميتها من كونها تنتمي إلى البحوث الحديثة المرتبطة بالأمن السيبراني والاتصال الرقمي في السياق الجامعي الجزائري، وتساهم في إثراء المكتبة الأكاديمية العربية بدراسة ميدانية تطبيقية في مجال ناشئ متزايد الأهمية.

وتعد الدراسة مهمة على المستوى التشخيصي، حيث تساعد في تقييم مستوى الوعي الرقمي لدى فئة استراتيجية من الطلبة، وهم طلبة الإعلام الآلي الذين يُتوقع أن يكونوا رواداً في نشر الثقافة السيبرانية مستقبلاً، كما تكشف العلاقة بين التكوين الأكاديمي التقني والسلوك الأمني، وهو ما يعزز الفهم النظري للعلاقة بين المعرفة التخصصية والسلوك الأمني الفعلي.

وتوفر الدراسة نتائج يمكن الاستفادة منها لتطوير البرامج التكوينية الجامعية في قسم الإعلام الآلي، واقتراح تعديلات على المقررات الدراسية لإدماج مفاهيم الأمن السيبراني بشكل منهجي. كما تساهم الدراسة، من خلال تحديد مستوى الوعي الحالي والممارسات الرقمية غير الآمنة، في وضع استراتيجيات وقائية تقلل من تعرض الطلبة للجرائم الإلكترونية والتهديدات السيبرانية، حماية للفرد والمؤسسة على حد سواء.

ب) الأهداف:

- تقييم مستوى الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي بجامعة محمد بوضياف بالمسيلة.
- التعرف على الأبعاد المعرفية والسلوكية والإدراكية للوعي الرقمي لدى الطلبة وتحديد الفجوات المعرفية لديهم.
- رصد المصادر الرئيسية لاكتساب الوعي بالأمن السيبراني لدى الطلبة.
- وصف وتحليل الممارسات والسلوكيات الرقمية لدى الطلبة ومدى توافقها مع معايير الأمن السيبراني.
- إبراز دور الجامعة في تعزيز الثقافة السيبرانية واقتراح آليات عملية لتعزيز الأمن السيبراني في الوسط الجامعي

4) أسباب اختيار الموضوع

أ) الأسباب الذاتية :

اختيار موضوع الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي جاء بناءً على اهتمام شخصي بمجال التكنولوجيا والمعلومات، ورغبة في فهم طبيعة التحديات الرقمية التي يواجهها الطلبة في البيئة الجامعية. كما ينبع هذا الاهتمام من الخبرة المباشرة في التعامل مع الوسائط الرقمية وملاحظة مدى تعرض الطلبة لمخاطر سيبرانية مختلفة، وهو ما حفز الباحث على دراسة العلاقة بين المعرفة الأكاديمية والسلوك الرقمي الواقعي. إضافة إلى ذلك، يعد الموضوع فرصة لتطوير مهارات البحث والتحليل في مجال ناشئ وذو أهمية متزايدة، مما يمثل حافزاً شخصياً لإثراء الفهم الذاتي والمهني في الأمن السيبراني.

ب) الأسباب الموضوعية

أما الأسباب الموضوعية فتكمن في أهمية الموضوع على المستوى الأكاديمي والمجتمعي، حيث يشهد العالم الجرائري توسعاً كبيراً في استخدام الإنترنت والوسائط الرقمية، مع تزايد ملحوظ في التهديدات السيبرانية، مثل الاختراقات، التصيد الاحتيالي، والجرائم الإلكترونية، مما يجعل دراسة الوعي الرقمي لدى طلبة الإعلام الآلي ضرورة ملحة. كما أن الموضوع يساهم في سد فجوة معرفية موجودة في البحوث المحلية حول العلاقة بين التكوين الأكاديمي في الإعلام الآلي والسلوكيات الأمنية للطلبة، ويقدم بيانات ميدانية يمكن الاعتماد عليها في تطوير برامج تكوينية وتعليمية ترفع مستوى الثقافة السيبرانية في الجامعات.

5) منهج الدراسة وأدواتها :

أ) منهج الدراسة

تعتمد هذه الدراسة المنهج الوصفي التحليلي (Descriptive Analytical Method) لكونه الأنسب لطبيعة الظاهرة المدروسة، فالمنهج الوصفي يتيح وصف الظاهرة كما هي في واقعها، من خلال رصد مستوى الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي، وتحديد خصائصها وسماتها. بينما يتيح المنهج التحليلي فحص العلاقات بين المتغيرات (كالعلاقة بين المستوى الدراسي والوعي الأمني، أو بين المصادر المعرفية والممارسات السلوكية)، وتفسير الأسباب والدوافع الكامنة وراء السلوكيات الرقمية الملحوظة.

ب) أدوات جمع البيانات

-الاستبيان (الأداة الرئيسية):

يعد الاستبيان أحد أدوات جمع البيانات والمعلومات الشائعة الاستخدام من قبل الباحثين الدراسات الاجتماعية خاصة منها تلك الدراسات الوصفية التي تتجه لتحليل الظاهرة المدروسة ومحاولة اكتشاف مختلف جوانبها.

تحتوي استمارة بحثنا على مجموعة من الأسئلة البسيطة والواضحة وقد بلغ عددها (31)سؤالا ، تمت صياغتها بما يتلاءم مع مستوى المبحوثين وبما يساهم في تسهيل عملية الإجابة ، وقد تم توزيع هذه الأسئلة على خمسة محاور رئيسية لتغطية أهداف الدراسة وهي كالآتي :

• **المحور الأول:** مستوى المعرفة بالأمن السيبراني، ويهدف هذا المحور إلى قياس حصيلة الطلبة المعرفية بالمفاهيم الأساسية للأمن السيبراني.

• **المحور الثاني:** مصادر الوعي بالأمن السيبراني، ويهدف هذا المحور إلى الكشف عن القنوات والمصادر التي يعتمد عليها الطلبة في اكتساب معرفتهم حول الأمن السيبراني.

• **المحور الثالث:** الممارسات والسلوكيات الرقمية للطلبة، ويسعى هذا المحور لرصد السلوكيات الميدانية للطلبة أثناء تعاملهم مع الفضاء الرقمي وتقييم مدى التزامهم بالإجراءات الوقائية.

• **المحور الرابع:** إدراك التهديدات السيبرانية وانعكاساتها، ويهدف هذا المحور لقياس مدى وعي الطلبة بطبيعة التهديدات والمخاطر السيبرانية المعاصرة وانعكاساتها.

• المحور الخامس: تقييم دور الجامعة وسبل التعزيز، ويختص هذا المحور باستكشاف واقع التكوين الجامعي المقدم للطلبة في هذا المجال، وتعميق البحث في مقترحاتهم حول آليات تطوير دور المؤسسة الجامعية في مواكبة التطورات التقنية.

-6- مجتمع الدراسة والعينة:

أ) مجتمع الدراسة:

مجتمع الدراسة (Population) هو مجموعة الأفراد أو الوحدات التي تشترك في سمة معينة ويستهدف البحث دراستها، في هذه الدراسة، يتكون مجتمع الدراسة من طلبة الإعلام الآلي، قسم الإعلام الآلي المسجلين بجامعة محمد بوضياف المسيلة وتحديدًا طلبة السنة أولى ماستر حيث بلغ العدد الإجمالي للمجتمع الأصلي (86) طالباً وطالبة مسجلين بصفة رسمية ومنتظمة، ويتوزع هذا الحجم الكلي على التخصصات المتاحة بالقسم وهي تخصص ذكاء اصطناعي وتخصص هندسة البرمجيات وأنظمة المعلومات، ليشكل هذا المجتمع بمجموعه القاعدة الأساسية والشاملة التي سُحبت منها عينة الدراسة الميدانية .

-7- خصائص مجتمع الدراسة:

- الخصائص التنظيمية: طلبة نظام (LMD) في تخصص دقيق هو الإعلام الآلي.
- الخصائص المكانية: المقيمون بالجامعة أو المنتسبون إليها بشكل منتظم.
- الخصائص الزمانية: الطلبة الذين يدرسون بالموسم الجامعي 2026/2025 م.

ب) عينة الدراسة :

-اختيار العينة:

نظراً لصعوبة دراسة جميع أفراد مجتمع الدراسة، ونظراً لطبيعة الموضوع تم الاعتماد على العينة القصدية (purposive sample) حيث يتم اختيار أفراد العينة بشكل عمدي وفق معايير يحددها الباحث بما يتلائم مع طبيعة موضوع الدراسة وأهدافها .

- حجم العينة:

يُحدد حجم العينة بناءً على مدى توفر الأفراد الذين تنطبق عليهم معايير الاختيار مع مراعاة قدرة الباحث على الوصول إليهم

وكذا استعدادهم للمشاركة في الدراسة بما يضمن تحقيق أهداف البحث والوصول الى نتائج ذات دلالة .

وتطبيقاً لذلك، ونظراً لظروف الاستجابة والتفاعل مع أداة الدراسة (الاستبيان)، استقرت العينة النهائية المستجيبة والتي خضعت فعلياً للتحليل الإحصائي عند (50) طالباً وطالبة، حيث توزعت هذه العينة ميدانياً حسب التخصصات الأكاديمية المكونة لها فبلغ عدد طلبة تخصص ذكاء اصطناعي (22) طالباً وطالبة، في حين بلغ عدد الطلبة المستجيبين في تخصص هندسة البرمجيات ونظم المعلومات (28) طالباً وطالبة من إجمالي العينة الخاضعة للدراسة .

- معايير شمول العينة :

- أن يكون الطالب مسجلاً رسمياً في قسم الإعلام الآلي

- أن يكون منتظماً خلال فترة إجراء الدراسة

- أن يوافق على المشاركة في الدراسة طوعاً.

(8) حدود الدراسة:

كل دراسة علمية ترتبط بحدود تحدد نطاقها وتضمن دقة نتائجها، ويمكن تقسيم حدود هذه الدراسة كالتالي:

أ) الحدود الزمانية

- تُجرى الدراسة خلال الفترة الممتدة من مارس 2026 إلى ماي 2026م.

ب) الحدود المكانية

- تقتصر الدراسة على جامعة محمد بوضياف المسيلة - قسم الإعلام الآلي " ماستر1"، دون التمدد إلى جامعات أخرى أو أقسام أخرى داخل نفس الجامعة.

(9) مصطلحات الدراسة

مفهوم الأمن السيبراني:

الأمن لغة : مشتق من كلمة (أَمِنَ) وهو نقيض الخوف فالأمن والأمان ، والأمانة ، والمنة تعني الطمأنينة ، لذا يقال آمن فلان يأمن آمنا، وأمنا إذا لم يخف¹ .

أما السببرانية لغة : (cyber) تطلق على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السببراني، والفضاء الإلكتروني . بمعنى التوجه أو القائد² .

التعريف الاصطلاحي:

يمكن وصف الأمن السببراني بأنه حماية الشبكات والانظمة المعلوماتية، بالإضافة الى البيانات والمعلومات والاجهزة المرتبطة بالانترنت .

وبالتالي هو المجال الذي يتضمن الإجراءات والمعايير والقياسات اللازمة للتعامل مع التهديدات ومنع التعديات ، او تقليل تأثيراتها في أوسع الظروف³ .

التعريف الإجرائي :

هو كل ما يفعله الفرد من إجراءات لحماية البيانات الرقمية من الاختراقات والتهديدات.

-مفهوم الشباب الجامعي:

لغة : يعرف الشباب في اللغة بأنه الفتوة والفتاء والحداثة ، بمعنى الحيوية والقوى الدينامية⁴ .
اما الجامعي فهو مأخوذ من كلمة الجامعة ، وتعني التجمع والقراءة⁵ .

التعريف الاصطلاحي :

¹ مصطفى محمد منجود، الأبعاد السياسية لمفهوم الأمن في الإسلام (القاهرة: المعهد العالمي للفكر الإسلامي، 1996) ص 30.

² سيناء علي محمود، "التحديات الأمنية للدول في الفضاء السببراني"، مجلة قضايا سياسية، جامعة النهريين، العدد 80، 313: (2024)

³ أحمد حاتم جبار عطية، "الأبعاد القانونية والاجتماعية للأمن السببراني"، مجلة الشرق الأوسط للدراسات القانونية والفقهية، المجلد 5، العدد 3 (2025): 441 .

⁴ حسيبة لولي، "الشباب ومظاهر التغير في ظل العولمة"، دراسات اجتماعية، العدد 18 (بدون تاريخ): 72.

⁵ العربي بن حمار صدام ورفاع محمد، "شبكات التواصل الاجتماعي وأثرها على القيم الدينية لدى الطلبة الجامعيين: دراسة وصفية حول استخدام الطلبة الجامعيين لشبكات التواصل الاجتماعي" (مذكرة ماستر، جامعة عبد الحميد بن باديس، 40: (2014/2015).

الشباب الجامعي هم فئة في مرحلة عمرية حيوية يعيشون تجربة التعليم العالي حيث يكتسبون معارف جديدة ويطورون مهاراتهم الفكرية والاجتماعية ، وهم في طور بناء الهوية وتحديد المسار المهني¹ .

التعريف الإجرائي :

يقصد بهم الطلبة المسجلين في الجامعة.

- مفهوم انتهاكات الخصوصية:

لغة : مصدر الفعل (إنتَهَكَ) ويعني التجاوز والتعدي على الحرمات اما الخصوصية تعني الصفة الموحدة في شيء ولا توجد في غيره².

انتهاك الخصوصية تعني التطفل على الحياة الخاصة او معلومات شخص اخر³.

التعريف الاصطلاحي :

وتعني التعدي على خصوصيات الآخرين والتدخل فيها دون موافقة منهم ويتم ذلك من خلال تقنيات تكنولوجيا متخصصة مثل اختراق البريد الالكتروني او التجسس على البيانات الشخصية وغيرها⁴.

التعريف الاجرائي :

الاطلاع على خصوصيات الآخرين دون علم منهم او اذن منهم .

مفهوم تطبيقات الإعلام الرقمي :

لغة : التطبيقات في اللغة هي جمع (تطبيق)، وهو من الفعل (طَبَّقَ) ومعناه وضع الشيء على الشيء أو جعله مطابقاً له اما الاعلام هو مصدر أَعْلَمَ ، بمعنى الاخبار وتبادل المعلومات ، اما الرقمي فهو نسبة الى الرقم⁵ .

¹ عوالمية إكرام وآخرون "الثقة بالنفس وعلاقتها بالتوجه نحو الحياة لدى الشباب الجامعي: دراسة ميدانية على عينة من طلبة كلية العلوم الإنسانية والاجتماعية بجامعة 8 ماي 1945 قالمة" (مذكرة ماستر، جامعة 8 ماي 1945 قالمة، 2024/2025):7.

² معجم المعاني الجامع، "انتهاك"، مادة لغوية، <https://www.almaany.com/ar/dict/ar-ar/انتهاك/>

³ إيرث، ماريا، وكيمبرلي وينستون. "انتهاك الخصوصية | التعريف والأنواع والأمثلة". تاريخ الاطلاع 9 ماي 2026. متاح على الرابط <https://study.com/academy/lesson/what-is-invasion-of-privacy-definition-examples.html>

⁴ عباس آمنة وخلف الله رانية، "وعي الطلبة الجامعيين الجزائريين بمخاطر انتهاك الخصوصية في البيئة الرقمية: دراسة ميدانية على عينة من طلبة علوم الإعلام والاتصال وعلم المكتبات جامعة قالمة" (مذكرة ماستر، جامعة 8 ماي 1945 قالمة، 2023/2022): 29 .

⁵ معجم المعاني الجامع، "الاعلام"، <https://www.almaany.com/ar/dict/ar-ar/>

ويشير المصطلح الى الوسائل المستخدمة لنقل المعلومات عبر الانظمة التقنية .

التعريف الاصطلاحي

تطبيقات الإعلام الرقمي هي الأدوات التي تستخدمها الشركات والمؤسسات للتواصل مع جمهورها عبر الإنترنت وتشمل هذه التطبيقات العديد من الخدمات والمنصات التي تساعد على نشر المحتوى الرقمي وتحسين تجربة المستخدمين¹.

التعريف الإجرائي:

هي التطبيقات والمنصات التي تُستخدم عبر شبكة الإنترنت والوسائط المتعددة لنقل المحتوى الإعلامي.

تعريف الوعي بالأمن السيبراني :

الوعي لغة : يعود لفظ وعي في العربية الى الجذر الثلاثي (و ع ي) بمعنى الحفظ والفهم والاستيعاب ، ووعي الشيء أي حفظ القلب الشيء².

التعريف الاصطلاحي : درجة الفهم من المستخدمين حول أهمية أمن المعلومات ومسؤولياتهم عن ممارسة مستويات كافية من مراقبة أمن المعلومات لحماية البيانات المنظمة والشبكات على نطاق واسع³.

التعريف الإجرائي :

يعني فهم و معرفة طرق الحماية من الاختراقات والجرائم الإلكترونية .

- أنواع الوعي بالأمن السيبراني:

- الوعي الرقمي بالأمن السيبراني:

هو مستوى إدراك المستخدم للمفاهيم والمعلومات الأساسية المرتبطة بالأمن السيبراني، مثل حماية البيانات والخصوصية الرقمية، وأنواع التهديدات الإلكترونية، وكيفية تأمين الحسابات.

- الوعي السلوكي بالأمن السيبراني:

¹ محمود الخطيب، "ما هي تطبيقات الإعلام الرقمي؟"، منصة تواصل، 19 أكتوبر 2022،

<https://tawasulforum.org/.....> ، تاريخ الاطلاع : 9 ماي 2026.

² ابن منظور ،محمد بن مكرم ،لسان العرب ،ط 3(بيروت ،دار صادر ،1414هـ) مجلد 15 ، ص 396.

³ أحمد مصطفى محمد أحمد القوسي، "فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى عينة من المراهقين مستخدمي الإنترنت بمدينة جدة"، مجلة الإرشاد النفسي، المجلد 78، العدد 2 (أبريل 2024):

هو مستوى التزام المستخدم بالممارسات والسلوكيات الرقمية الآمنة أثناء استخدام المنصات الرقمية، مثل اختيار كلمات مرور قوية، وتجنب الروابط المشبوهة، وضبط إعدادات الخصوصية.

- الوعي المهني بالأمن السيبراني:

هو مستوى وعي المستخدم بالمسؤوليات المهنية المرتبطة بالأمن السيبراني في الممارسات الإعلامية الرقمية، بما يشمل التحقق من صحة المعلومات، وتجنب نشر المحتوى المضلل، والالتزام بأخلاقيات العمل الإعلامي في البيئة الرقمية.

- الوعي بالخصوصية والمسؤولية الرقمية:

هو مستوى إدراك المستخدم لأهمية حماية الخصوصية الرقمية واحترام حقوق الآخرين عند استخدام المنصات الرقمية، والالتزام بالمسؤولية القانونية والأخلاقية في تداول المحتوى، كما يشمل احترام قواعد النشر.

- دور التعليم الإعلامي في تعزيز الوعي بالأمن السيبراني:

هو مدى إسهام التعليم الإعلامي والمقررات الأكاديمية في توعية الطلبة بالأمن السيبراني، وتطوير مهاراتهم في الاستخدام الآمن والمسؤول للمنصات الرقمية.

-10- المقاربات النظرية للدراسة :

تعتبر النظريات السلوكية والاتصالية بمثابة القاعدة الأساسية التي يُعتمد عليها لفهم وتفسير طريقة تعامل المستخدمين مع قضايا الحماية والأمن الرقمي إذ تساعد هذه الأطر في توضيح كيفية تشكّل الوعي بالمخاطر السيبرانية وتفسير ردود أفعال الأفراد لحماية خصوصيتهم وبياناتهم من التهديدات المختلفة، وعليه تهدف دراستنا الحالية إلى استخدام مدخل نظري يساعدنا على فحص ظاهرة "الوعي بالأمن السيبراني وسلوك الحماية" من جوانبها المعرفية والنفسية، ولتحقيق هذا الهدف تم الاعتماد على النظريات التالية:

1. نظرية حماية الدافع (Protection Motivation Theory – PMT)

- تعد نظرية حماية الدافع من النظريات السلوكية الرائدة التي تبحث في كيفية إدراك الأفراد للمخاطر وتطوير استجابات حمائية ضدها في البيئات الافتراضية والواقعية¹
- تفترض هذه النظرية أن دافع الطالب لحماية بياناته الشخصية عبر تطبيقات الإعلام الرقمي يتشكل عبر مسارين معرفيين هما: تقييم التهديد وتقييم الاستجابة².
- ففي مسار "تقييم التهديد"، يدرك طالب الإعلام الآلي مدى شدة خطورة الهجمات السيبرانية (البرمجيات الخبيثة والتصيد) ومدى احتمالية تعرضه الشخصي لها أثناء تصفحه اليومي. (Rogers, 1975).
- أما في مسار "تقييم الاستجابة"، فيقوم الطالب بتقييم مدى فاعلية إجراءات الأمان المتوفرة (التشفير وتغيير كلمات المرور)، ومدى ثقته في قدرته التقنية الذاتية على تطبيقها لمنع الاختراق.

2. نموذج قبول التكنولوجيا (Technology Acceptance Model – TAM)

- يركز نموذج قبول التكنولوجيا على تفسير العوامل التي تحكم سلوك الأفراد وفئات المستخدمين عند التعامل مع الأنظمة الرقمية وأدوات الحماية التقنية والبرمجيات الأمنية.
- يركز النموذج على محددتين أساسيتين يفسران وعي الطالب وسلوكه؛ المحدد الأول هو "الفائدة المدركة" ويقصد بها مدى إدراك الطالب بأن استخدام جدران الحماية وبرامج الأمان سيعزز سلامة بياناته .
- أما المحدد الثاني فهو "سهولة الاستخدام المدركة"، ويعني مدى رؤية الطالب بأن تطبيقات الأمان الرقمي سلسلة وغير معقدة، وهو محدد يتأثر إيجاباً بالخلفية المعرفية لطلبة الإعلام الآلي ووفقاً للنموذج، فإن التفاعل بين الفائدة المدركة والسهولة هو الذي يشكل الاتجاه السلوكي الفعلي لدى الشباب الجامعي نحو الالتزام التام بمعايير الأمن السيبراني .

3. المقاربة المعرفية السلوكية في البيئة الرقمية (Cognitive–Behavioral Approach)

- تنطلق هذه المقاربة من فرضية أن سلوك الفرد في الفضاء الافتراضي هو نتاج مباشر لعمليات الإدراك والمعرفة التي يكتسبها في بيئته المحيطة والتعليمية .

¹ Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

<https://doi.org/10.1080/00223980.1975.9915803>

² Rogers, R. W., & Prentice–Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), Handbook of health behavior research I: Personal and social determinants (pp. 113–132). Plenum Press.

- تبحث المقاربة في العلاقة التفاعلية بين ثلاثة أبعاد رئيسية: المعرفة الأمنية النظرية، والاتجاهات والقيم الرقمية، والممارسات السلوكية التطبيقية للمستخدم¹.
- وفي إطار هذه الدراسة، تسعى المقاربة إلى تفسير كيفية انتقال طالب الإعلام الآلي من مرحلة "الوعي المعرفي والأكاديمي" الذي يتلقاه في مدرجات الجامعة، إلى مرحلة "الوعي السلوكي" وتجسيده في تدابير وقائية واقعية.
- وتساعد هذه المقاربة في رصد الفجوة المنهجية بين ما يملكه الطالب من مخزون معرفي تقني، وبين ممارساته الميدانية الحقيقية في مواجهة انتهاكات الخصوصية.

1- الدراسات السابقة

أ) الدراسات السابقة الوطنية²:

عنوان الدراسة: مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية لدى مستخدمي الإنترنت في الجزائر: دراسة ميدانية على طلبة الجامعات

ملخص الاشكالية: هدفت إلى تحديد مستوى الوعي بالأمن السيبراني لدى طلبة الجامعات في الجزائر، وذكرت أن الوعي كان بدرجة متوسطة، مع حاجة لتعزيز التدريبات الوقائية. مجتمع البحث: طلبة الجامعات الجزائرية.

• **العينة:** عينة من طلبة الجامعات (مستخدمو الانترنت)

• **منهج البحث :** المنهج الوصفي.

• **أدوات جمع البيانات:** استمارة استبيان.

• **أهم النتائج:** خلصت الدراسة إلى أن مستوى الوعي كان بدرجة متوسطة، مع وجود حاجة ملحة لتعزيز التدريبات الوقائية والعملية³.

¹ محمد، عبد الفتاح. (2021). سوسيولوجيا الشباب الجامعي في العصر الرقمي. المكتب الجامعي الحديث.

² برادة، عبد الرزاق، ودحماني، فاطمة. (2024). مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية لدى مستخدمي الإنترنت في الجزائر: دراسة ميدانية على طلبة الجامعات. مجلة البحوث والدراسات الإعلامية، جامعة الجزائر، 12(2)، 45-68

³ ثابت، مصطفى، وبوعكاز، حدة، وربوح، عبلة. (2022). وعي الطالب الجامعي بالأمن السيبراني ومخاطر انتهاك الخصوصية عبر شبكات التواصل الاجتماعي - حالة طلبة جامعة قاصدي مرباح ورقلة. مجلة الاتصال والمجتمع، جامعة ورقلة، 6(1)، 112-135.

عنوان الدراسة: وعي الطالب الجامعي بالأمن السيبراني ومخاطر انتهاك الخصوصية عبر شبكات التواصل الاجتماعي – حالة طلبة جامعة قاصدي مرباح ورقلة

ملخص الإشكالية : درست وعي الطلاب بمخاطر الخصوصية والأمن السيبراني، وأظهرت أن الوعي محدود نسبياً في بعض الجوانب، مع ضعف في إجراءات الحماية الرقمية.

مجتمع البحث: طلبة جامعة قاصدي مرباح ورقلة.

• **العينة:** عينة قصدية من طلبة الجامعة.

• **منهج البحث:** المنهج الوصفي التحليلي.

• **أدوات جمع البيانات:** استمارة استبيان.

• **أهم النتائج:** أظهرت النتائج أن وعي الطلاب بمخاطر الخصوصية محدود نسبياً في بعض الجوانب، مع وجود ضعف في تطبيق إجراءات الحماية الرقمية الفعلية¹.

عنوان الدراسة: الوعي بالأمن السيبراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال – دراسة تطبيقية في جامعة الشهيد حمه لخضر بالوادي

ملخص الإشكالية: تناولت مدى دراية طلبة الإعلام بالتهديدات السيبرانية وأساليب حماية المعلومات الرقمية في ظل التطور التكنولوجي .

مجتمع البحث: طلبة جامعة الشهيد حمه لخضر بالوادي.

• **العينة:** طلبة قسم علوم الإعلام والاتصال.

• **منهج البحث:** المنهج الوصفي (دراسة تطبيقية).

• **أدوات جمع البيانات:** استمارة استبيان.

• **أهم النتائج:** خلصت الدراسة إلى وجود وعي متوسط لدى طلبة الإعلام بالتهديدات السيبرانية وأساليب الحماية.

¹ عزيزي، سمير، وسلامة، يوسف الصديق. (2025). الوعي بالأمن السيبراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال – دراسة تطبيقية في جامعة الشهيد حمه لخضر بالوادي. المجلة الجزائرية لبحوث الاتصال، جامعة الوادي، 9(1)، 89-105.

ب - الدراسات السابقة الدولية¹:

عنوان الدراسة: دور الوعي بالأمن السيبراني في عصر التحول الرقمي - دراسة تطبيقية في المجتمع الجزائري

ملخص الاشكالية: ركزت على علاقة الوعي السيبراني بالتحول الرقمي في المجتمع وأكدت أهمية تعزيز الثقافة الوقائية في البيئة الرقمية.

• مجتمع البحث: المجتمع الجزائري.

• العينة: عينة من مستخدمي التكنولوجيا في المجتمع الجزائري.

• منهج البحث: المنهج الوصفي.

• أدوات جمع البيانات: استمارة استبيان.

• أهم النتائج: أكدت الدراسة على أهمية ربط الوعي السيبراني بمفاهيم التحول الرقمي وضرورة تعزيز الثقافة الوقائية لدى أفراد المجتمع.

عنوان الدراسة: الأمن السيبراني والإعلام الرقمي: انعكاسات التدخلات الرقمية على الأمن الأسري والمجتمعي - دراسة ميدانية في جامعة بغداد

ملخص الاشكالية: بحثت تأثير استخدام الوسائط الرقمية غير الواعي على الأمن الأسري والمجتمعي، وأهمية نشر الوعي السيبراني للحد من المخاطر.

مجتمع البحث: طلبة جامعة بغداد.

• العينة: عينة من طلبة الجامعة.

• منهج البحث: المنهج الوصفي الميداني.

• أدوات جمع البيانات: استمارة استبيان.

• أهم النتائج: أظهرت وجود انعكاسات مباشرة للاستخدام غير الآمن للوسائط الرقمية على الأمن الأسري، وأكدت على أهمية دور الإعلام في نشر الوعي السيبراني.

عنوان الدراسة: درجة إلمام طلبة كلية التربية بجامعة دمشق بمفاهيم الأمن السيبراني - دراسة ميدانية تحليلية

¹ موسى، مروة، ومصطفى، عبد اللطيف، ونادر، محمود فواز. (2025). دور الوعي بالأمن السيبراني في عصر التحول الرقمي - دراسة تطبيقية في المجتمع الجزائري. مجلة التنمية والتحول الرقمي، 4(2)، 15-32.

ملخص الاشكالية : هدفت إلى قياس مستوى إدراك الطلاب لمفاهيم الأمن السيبراني، وأكدت أن الوعي لا يزال في حاجة إلى تعزيز من خلال التدريب والتكوين.

• مجتمع البحث: طلبة كلية التربية بجامعة دمشق.

• العينة: عينة من طلبة الكلية.

• منهج البحث: المنهج الوصفي التحليلي.

• أدوات جمع البيانات: استمارة استبيان.

• أهم النتائج: بينت الدراسة أن مستوى إدراك الطلاب لمفاهيم الأمن السيبراني لا يزال يحتاج إلى دعم من خلال التكوين والتدريب الأكاديمي المتخصص.

-التعقيب على الدراسات السابقة:

أظهرت الدراسات السابقة تنوعاً في نتائج وعي الطلاب بالأمن السيبراني. ففي الجزائر، أظهرت دراسة برادة ودحماني (2024) بعنوان «مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية لدى مستخدمي الإنترنت في الجزائر: دراسة ميدانية على طلبة الجامعات» أن الوعي السيبراني لدى الطلبة كان بدرجة متوسطة، مع حاجة واضحة لتعزيز التدريبات العملية وفي نفس السياق، تناولت دراسة ثابت وبوعكاز وروبوح (2022) موضوع «وعي الطالب الجامعي بالأمن السيبراني ومخاطر انتهاك الخصوصية عبر شبكات التواصل الاجتماعي - حالة طلبة جامعة قاصدي مرباح ورقلة» الارتباط بين استخدام الشبكات الاجتماعية ومخاطر انتهاك الخصوصية، وأكدت وجود وعي محدود بإجراءات الحماية الرقمية. كما كشفت دراسة سمير وعزيزي (2025) بعنوان «الوعي بالأمن السيبراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال - دراسة تطبيقية في جامعة الشهيد حمه لخضر بالوادي» عن وعي متوسط لدى طلبة الإعلام بالتهديدات السيبرانية وأساليب الحماية.

-ومن خلال استقراء الدراسات السابقة الوطنية منها والدولية، أمكننا تحديد ملامح التقاطع والتباعد بين تلك الجهود والدراسة الحالية وفق الآتي:

1. من حيث أوجه التشابه:

نلاحظ أن دراستنا تلتقي مع التوجه العام للدراسات الميدانية الحديثة، وخاصة دراسة (برادة ودحماني، 2024) ودراسة (ثابت وبوعكاز، 2022)، في اختيار "الطالب الجامعي" كعينة محورية؛ وهذا مبرر منطقي لكون هذه الفئة هي الأكثر انغماساً في البيئة الرقمية. كما تتفق دراستنا منهجياً مع ما ذهب إليه (عزيزي وسلامة، 2025) في استخدام المنهج الوصفي، كونه الأنسب لتوصيف ظاهرة الوعي وتحليل ممارسات الحماية لدى المستخدمين.

2. من حيث أوجه الاختلاف (الفجوة البحثية):

رغم هذا التقاطع، إلا أن دراستنا الحالية تحاول التخصص بشكل أدق في "تطبيقات الإعلام الرقمي" (مثل شبكات التواصل الحديثة)، بينما اتسمت دراسات أخرى مثل دراسة (مويسي وآخرون، 2025) بالشمولية في تناول التحول الرقمي بصفة عامة.

بالمقابل، نجد أن دراستنا تذهب أبعد من مجرد قياس الوعي (كما في دراسة بكور، 2025)، لتسلط الضوء على "انعكاسات انتهاك الخصوصية" تحديداً، وهو ربط نرى أنه يمثل فجوة علمية لم تشبها الدراسات السابقة في البيئة الجامعية الجزائرية بالقدر الكافي، خاصة مع التطورات التقنية المتسارعة في سنة 2026.

الفصل الثاني

(ماهية الأمن السيبراني)

تمهيد

تُعد الدراسة النظرية والمفاهيمية المنطلق الأساسي الذي يمنح البحث العلمي قيمته المعرفية فلا يمكن ملامسة الواقع الميداني لأي ظاهرة دون الاستناد إلى إطار معرفي يمكن الباحث من ضبط متغيراتها وفهم أبعادها والحدود الفاصلة بين مصطلحاتها ، وهنا يأتي الأمن السيبراني بوصفه المتغير الأساسي لحماية وتأمين الممارسات الرقمية إذ إن تعزيز الوعي الرقمي لم يعد يقتصر على الجانب المعرفي فحسب بل أصبح ضرورة سلوكية تستلزم بناء ثقافة أمان تضمن حماية المستخدمين.

ومن خلال هذا الطرح، يسعى هذا الفصل إلى الإحاطة بالمفاهيم المتعلقة بالأمن السيبراني ليوفر أرضية نظرية متماسكة تجمع بين الجانب التقني للأمن الرقمي والجانب السلوكي للمفاهيم المدروسة مما يسهل عملية قراءة المؤشرات الميدانية وتفسيرها بطريقة علمية دقيقة.

ويتألف هذا الفصل من مبحثين متكاملين ومتداخلين، يُعالج كلٌّ منها بُعداً أساسياً من أبعاد الدراسة؛ حيث يدرس المبحث الأول الأمن السيبراني وأبعاده النظرية، مقدماً استعراضاً نظرياً للمفاهيم والخصائص المرتبطة بهذا الفضاء الرقمي، بينما يخصص المبحث الثاني الحديث عن الوعي بالأمن السيبراني في الوسط الجامعي من حيث المفهوم والأهمية، بالإضافة إلى تتبع دور الجامعة والإستراتيجيات المعتمدة في تعزيزه لدى الطلبة.

المبحث الأول: الأمن السيبراني وأبعاده النظرية

أدى التطور الهائل في تكنولوجيا المعلومات والاتصالات إلى الاعتماد على الفضاء الرقمي في تسيير مختلف الأنشطة، وهو الواقع الجديد الذي أفرز تحديات ومخاطر أمنية بالغة التعقيد تترصد بالأنظمة والبيانات وفي ظل هذه التحولات، أصبح مفهوم "الأمن السيبراني" ضرورة حتمية واستراتيجية دفاعية لا غنى عنها لضمان حماية الفضاء الافتراضي واستقرار مستخدميه.

المطلب الأول: ماهية الأمن السيبراني (المفهوم، النشأة، الخصائص)

1- تعريف الأمن السيبراني:

فهم الأمن السيبراني اليوم أصبح أمراً ضرورياً تسعى كثير من الدول والمؤسسات لتعزيزه لمواجهة التحديات المتزايدة في الفضاء الرقمي، حيث تطلق كلمة سيبراني (cyber) على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني، والفضاء الإلكتروني (Cyber space)، والأخير يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر الإنترنت، أو الشراء أونلاين وغيرها من الخدمات في جميع مجالات الحياة على مستوى العالم¹.

وفي ذات السياق، يمكن تعريف الأمن السيبراني على أنه مجموعة من المبادئ والممارسات التي تهدف إلى حماية المعلومات والأنظمة من الوصول غير المصرح به أو الأذى. ومع النمو السريع في التكنولوجيا أصبحت الشبكات المعلوماتية عرضة للعديد من التهديدات مثل الهجمات الإلكترونية والبرمجيات الضارة، مما يجعل تعزيز الأمن السيبراني أمراً مهماً لكافة الكيانات الحكومية والخاصة².

ومن منظور آخر، فإن الأمن السيبراني هو "ذلك الفرع الذي يهتم بحماية الشبكات والأنظمة المعلوماتية، والبيانات الحيوية التي تحتويها، بهدف حماية البيئة الافتراضية من كافة التهديدات المحتملة، سواء كانت تقنية ناتجة عن برمجيات خبيثة، أو غير تقنية ناتجة عن أخطاء بشرية، لضمان استمرار عمل النظم وحماية خصوصية المستخدمين³.

¹ سيناء علي محمود، "التهديدات الأمنية للدول في الفضاء السيبراني"، مجلة قضايا سياسية، جامعة النهريين، العدد 80 (2024): 313.

² علاء عبد الخالق حسين وآخرون، الأمن السيبراني: المبادئ والممارسات لضمان سلامة المعلومات (بغداد: دار السرد للطباعة والنشر والتوزيع، 2024)، 12.

³ عوفي مصطفى، أمن المعلومات والخصوصية الرقمية (عمان: دار اليازوري العلمية، 2022)، 113.

وحسب إيهاب خليفة الأمن السيبراني هو مجموعة الأدوات والسياسات والمفاهيم الأمنية ومناهج إدارة المخاطر والإجراءات وأفضل الممارسات والضمانات التكنولوجية التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصورة عامة¹.

ومن التعريفات التي تحدد إجراءات وسياسات الأمن السيبراني تعريف الاتحاد الدولي للاتصالات حيث يشير مصطلح 'الأمن السيبراني' إلى مجموعة شاملة من الأنشطة التي تهدف إلى حماية البيئة السيبرانية، وتتضمن تطبيق سياسات وإجراءات أمنية واعتماد مبادئ توجيهية وتبني مقاربات فعالة لإدارة المخاطر بالإضافة إلى تنفيذ برامج تدريبية واستخدام تقنيات حديثة لحماية أصول المؤسسات والمستخدمين².

ويمكن تعريف الأمن السيبراني بأنه أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية، المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأساء الأحوال. ويرتبط هذا الأمن، ارتباطاً وثيقاً، بأمن المعلومات، في الوصول إلى هذه الأخيرة، أو بثها، أو الاطلاع عليها والمتاجرة بها، أو تشويهاها واستغلالها، هو ما يقف، غالب الأحيان، وراء عمليات الاعتداء على الشبكات، وعلى الإنترنت. فالاعتماد على المعلومة، حقيقة لا لبس فيها، تفرض اعتماداً أكبر، على الأنظمة الإلكترونية التي تعالجها³.

وبهذا يمكن القول إن الأمن السيبراني هو مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة⁴.

-2- نشأة الأمن السيبراني:

ظهر مفهوم الأمن السيبراني بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة، وقد تم استخدامه لأول مرة من قبل علماء الكمبيوتر في أوائل التسعينيات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر، لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدون

¹ إيهاب خليفة، "الأمن السيبراني: الماهية والإشكاليات"، مجلة رؤى مصرية، المركز العربي للبحوث والدراسات، العدد 54 (أكتوبر 2019): 5.

² التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الإصلاح في الاتصال عام 2010-2011"

³ منى الأشقر جبور، السيبرانية هاجس العصر (بيروت: المركز العربي للبحوث القانونية والقضائية، 2016)، 2.

⁴ القانون رقم 04-18 المؤرخ في 10 مايو 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27 (13 مايو 2018): 7.

على أن التهديدات الناشئة عن التقنيات الرقمية من الممكن أن يكون لها عدة آثار اجتماعية مدمرة.¹ ، فالجرائم المعلوماتية تطورت بشكل كبير منذ الأيام الأولى في عمر شبكة الإنترنت ومع ازدياد الاعتماد عليها في أعمالنا اليومية والتحويلات المالية وتبادل الرسائل، أصبح مستوى الخطر أعلى بكثير مما كان عليه في ذلك الوقت، فقد تم إنشاء أول جهاز حاسب عام 1943 ولم تكن هذه الأجهزة متصلة عبر الشبكة ولم يكن هناك آليات الاتصال وتبادل البيانات والملفات، وهذا الأمر يعتبر مناخاً آمناً ولذلك كانت التهديدات الأمنية الرقمية شبه معدومة ولكن في أواخر هذا العقد طور الكثيرون نظرية الفيروسات من الاعتقاد القائل أن الكائنات الحية الميكانيكية يمكن أن تنسخ نفسها وتتكاثر وتقوم بعمل يؤدي لإتلاف الآلات، وبالفعل ظهرت ورقة بحثية عن هذا الموضوع لاحقاً في عام 1966.²

وفي الخمسينات، لم يتم تطوير عمليات الاختراق في البداية بهدف جمع المعلومات من خلال استخدام أجهزة الحاسب، وبدلاً من ذلك كانت جذور عمليات الاختراق قد ظهرت مع الاستخدام المبكر لأجهزة الهاتف في الخمسينات من القرن الماضي فقد سعى البعض للتلاعب بالبروتوكولات الموجودة بهدف إجراء مكالمات مجانية أو مكالمات دولية برسوم منخفضة ولم يكن لدى شركات الهاتف وسائل لمنع حدوث هذا الأمر لفترة طويلة ويُذكر أن Steve Jobs و Steve Wozniak مؤسساً شركة آبل كانا مهتمين بالقيام بهذه الأمور في ذلك الوقت، وكانت فترة الستينات قد جلبت معها العديد من الابتكارات في صناعة الحاسب وفي هذا العقد بدأ ظهور مصطلح الاختراق أو القرصنة ولم يأت في البداية مع استخدام أجهزة الحاسب بل كانت عندما قام مجموعة من الأشخاص باختراق مجموعة تحكم بالقطارات بهدف تعديل مراكز وظائفهم ومن هنا كانت نقطة البداية لانتقال هذا الأمر إلى أجهزة الحاسب وكان هذا أحد الأحداث الرئيسية في عام 1967، حيث رحبت شركة IBM بمجموعة من الطلاب في مكاتبها لتجربة جهاز حاسب مصمم حديثاً، وتعلّم الطلاب اللغة الخاصة بنظام الحاسب وتمكنوا من الوصول إلى أجزاء مختلفة من النظام وقد قدم هذا الأمر لشركة IBM نظرة على نقاط الضعف الموجودة في النظام وكانت هذه الخطوة ذات أهمية كبيرة في تطوير استراتيجيات الأمن السيبراني وفي تلك الفترة لم يكن وضع أجهزة الحاسب في غرف مقفلة أمراً مجدياً أو مفيداً وكانت هذه الفترة هي البداية لاستخدام كلمات السر للوصول لأجهزة الحاسب.¹

وفي السبعينات تمت الولادة الحقيقية للأمن السيبراني وبدأ ذلك بمشروع يسمى شبكة مشاريع الأبحاث المتقدمة ARPANET والتي كانت عبارة عن شبكة للاتصال تم تطويرها قبل شبكة الانترنت وجد رجل يدعى

¹ سيناء علي محمود، مرجع سابق، ص 313.

Bob Thomas أنه من الممكن لبرنامج حاسب أن ينتقل عبر الشبكة بين محطات كانت تسمى Tenex وسمى هذا البرنامج Creeper وقد أنشأ توماس هذا البرنامج ليقوم بطباعة رسالة بسيطة وهي "I'm the creeper catch me if you can" حيث أثار هذا البرنامج الكثير من الاهتمام وبعض القلق وكان هذا البرنامج والرسالة الخاصة به الدافع وراء قيام شخص يدعى Ray Tomlinson بتطوير برنامج جديد له الاسم Reaper وكان الهدف منه مطاردة وحذف رسائل البرنامج Creeper ، فالبرنامج الجديد Reaper يعتبر المثال الأول لبرنامج مضاد الفيروسات وكان يطلق عليه برنامج النسخ الذاتي وهذا الأمر جعله أول worm في عالم أنظمة الحاسب في تلك الفترة من الزمن استمرت تقنيات الحاسب بالتطور والنمو والتوسع واعتمدت معظم الشبكات على أنظمة الاتصال وأدى ذلك إلى مستوى أعلى من الطلب على طرق الحماية وتأمين الشبكات وخلقت كل قطعة من الأجهزة المتصلة بالشبكة نوعاً جديداً من نقاط الدخول وكانت عبارة عن نقاط ضعف في الشبكة.

وفي عام 1983 تم تطوير مصطلحات جديدة لوصف هذه الهجمات ومن بينها مصطلحات "فيروسات الحاسب" و"حصان طروادة" وشكل الخوف من التجسس الإلكتروني مخاوف كبيرة في تلك الفترة مما دفع الحكومة الأمريكية إلى إنشاء إرشادات وموارد جديدة، وقد تم تطوير معايير تقييم نظام الحاسب الموثوقة عام 1985 والذي سمي لاحقاً بالكتاب البرتقالي والذي يعتبر من أول أدلة الحماية والأمان لأنظمة الحاسب وفي تلك الفترة تم إطلاق بعض إجراءات الحماية الأساسية التي أدت لاحقاً لإنشاء الأساس الذي تم من خلاله تطوير برامج الحاسب التجارية الخاصة بالأمن السيبراني، ثم تحولت التهديدات لأمر حقيقي حيث تمكن هاجر من ألمانيا عام 1986 من التسلل لأنظمة الحكومة الأمريكية والوصول لحوالي 400 جهاز حاسب مخصص للاستخدامات العسكرية وبدأ العمل على تطوير الاستراتيجيات والإجراءات للتخفيف من هذه المخاطر وفي الجزء الأخير من هذا العقد بدأت عملية تطوير صناعة الأمن السيبراني حيث تم تطوير برامج مضادات الفيروسات التجارية وإصدارها لأول مرة عام 1987. وتوجد ادعاءات كثيرة حول تحديد أول منتج لمضاد الفيروسات ومن أبرزها VirusScan الذي طوره John McAfee ، كما تم إصدار منتجات أخرى مثل NOD في تشيكوسلوفاكيا¹.

¹ جميل حسين طويلة، "تاريخ الأمن السيبراني"، منصة Cyberpedia ، تاريخ الاطلاع 15 أبريل 2026، متاح على الرابط: <https://www.cyberpedia.site>

وفي فترة الثمانينيات ازدهرت عملية تطوير دودة الحاسب worm التي تنتقل عبر الشبكة وتتكاثر بشكل تلقائي، ويعد Robert T. Morris أول من طورها بهدف تحديد حجم الإنترنت، مما تسبب ببطء شديد وكان السبب الرئيسي وراء تطوير فرق الاستجابة للطوارئ للمعلوماتية.

ومع بداية التسعينات شهد هذا العقد نمواً وتطوراً كبيراً في شبكة الانترنت وتطور صناعة الأمن السيبراني، حيث تم تطوير أول كود فيروس قادر على التحول يعرف باسم الفيروس متعدد الأشكال لتجنب اكتشافه، كما ظهرت برامج خبيثة أصابت الملايين مثل Melissa و ILOVEYOU وتسببت في فشل أنظمة البريد الإلكتروني. وبحلول عام 2000 وصل نمو الشبكة لمعظم المنازل والمكاتب وظهرت طرق إصابة بمجرد الانتقال إلى موقع ويب، وتطورت مجموعات القرصنة التي أطلقت هجمات منع خدمة موزع DDoS مثل مجموعة Anonymous، بالإضافة لعمليات اختراق بطاقات الائتمان وهجمات ياهو المشهورة. أما في مرحلة ما بعد 2010 فقد أصبحت الهجمات التي ترعاها الدول هي محور القلق كسلاح فعال لجمع المعلومات، مثل هجوم مجموعة Lazarus Group على شركة Sony عام 2014، ومع استمرار تطور المهاجمين استمرت شركات الحماية بتطوير حلول مثل التحليل الجنائي الرقمي، المصادقة ذات العوامل المتعددة، وأنظمة كشف ومنع الاختراق¹.

إن هذا التدرج التاريخي يثبت أن الأمن السيبراني لم يعد مجرد إجراء تقني دفاعي بل تحول إلى ثقافة مؤسسية وعلم قائم بذاته، حيث انتقل من حماية الأجهزة (Hardware) في السبعينات، إلى حماية البرمجيات والشبكات في التسعينات، وصولاً إلى حماية السلوك البشري والوعي الرقمي في وقتنا الراهن.

3- خصائص الأمن السيبراني:

الأمن السيبراني يتسم بخصائص وسمات متنوعة تبين أنه ليس مسار عمل لمرة واحدة إنما هو نشاط مستمر يستلزم اعتماد آليات دفاع مبتكرة كما يعمل على توفير نظام بيئي سيبراني آمن وإنشاء نظام موثوق به، يعمل على الدفاع اللاحق والذي يتمثل في قاعدة إرجاع الوضع إلى ما كان عليه، وبالتالي يوفر خاصية التنبيه إلى وجود خلل أو سوء استخدام الشبكات التي تعرض البيانات والمعلومات إلى الخطر من داخل المؤسسات².

وبما أن الجريمة الإلكترونية تتم بمنهجية وأساليب جديدة ذات بعد تكنولوجي أعلى من الجرائم التقليدية كان لا بد أن يأتي الأمن السيبراني للتغلب على هذه المشكلة مواكب التطور التكنولوجي ولذا تميز بخصائص أخرى تمثلت في

:

¹ المرجع نفسه.

² محمد مصطفى محمد حمد وآخرون، "دور الأمن السيبراني في مواجهة المخاطر الإلكترونية"، المجلة العلمية لكلية التربية - جامعة أسيوط، المجلد 40، العدد 11 (نوفمبر 2024): 157

• الاكتشاف والتعقب: حيث يهدف الأمن السيبراني إلى اكتشاف الجريمة الإلكترونية وتعقب أثرها وبالتالي التغلب عليها.

• السرعة وغياب الدليل: فصعوبات أثبات الجرائم الإلكترونية نظراً لاستخدام المخترقين وسائل تقنية حديثة أتى الأمن السيبراني بتقنيات حديثة عالية تفوق خبرة المجرم¹.

• الوقاية من الفيروسات والبرامج الضارة: يتم ذلك من خلال استخدام أنظمة مكافحة الفيروسات والحماية من البرامج المؤذية وتحديث هذه البرمجيات بشكل دوري.

• التحقق من الهوية وإدارة الوصول: من خلال استخدام نظم التأكد من الهوية وإدارة الوصول لمواقع الإنترنت والشبكات الخاصة للشركات.

• التشفير والتوقيع الإلكتروني: من خلال توظيف تقنيات التشفير والتوقيع الرقمي للتأكد من سلامة البيانات وحمايتها من الاختراق والتغيير².

المطلب الثاني: عناصر الأمن السيبراني وأبرز تهديداته الرقمية

يستند الأمن السيبراني إلى مجموعة من العناصر الجوهرية التي تتكامل فيما بينها لحماية الأصول الرقمية، بدءاً من تأمين التطبيقات والشبكات وصولاً إلى الجانب التشغيلي والتعافي من الكوارث ، وفي المقابل تواجه هذه المنظومة الأمنية تحديات مستمرة تتمثل في تهديدات رقمية متنوعة ومعقدة تتطلب فهماً عميقاً لطبيعتها وآليات عملها لضمان كفاءة الانظمة.

1- العناصر الرئيسية للأمن السيبراني:

أ- أمن التطبيقات :

ويعني إبقاء البرامج والأجهزة خالية من المخاطر، حيث يوفر التطبيق المخترق وسيلة للوصول إلى البيانات المحمية. ويبدأ التأمين الناجح في مرحلة التصميم، قبل نشر البرنامج. ويتعلق أمان التطبيقات بالحفاظ على البرمجيات منيعة أمام التهديدات. ومن المسببات الأساسية لسوء تهيئة التطبيق السحابي هي:

-نقص الوعي بسياسات أمن السحابة.

- غياب ضوابط ورقابة كافية.

¹ جيهان سعد محمد الخضري وآخرون، "الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة"، مجلة تطوير الأداء الجامعي، المجلد 12، العدد 1 (أكتوبر 2020): 223.

² محمد مصطفى محمد حمد وآخرون، مرجع سابق، ص 157.

- استعمال الكثير من واجهات التحكم.

- سلوك إهمال من الداخل (على سبيل المثال، خطأ مستخدم).

- الإجراءات مثل إعداد ضوابط متعددة العوامل، وهي خطوات ستستخدمها خدمات استشارات الأمن السيبراني للمساعدة في تعزيز أمان التطبيق ومنع اختراقه.

ب- أمن المعلومات:

يغطي أمن المعلومات حماية بيانات المؤسسة والمعلومات التي تجمعها من العملاء أو البائعين. وتحتاج معظم الشركات إلى الالتزام بواحد أو أكثر من معايير أمن المعلومات، ويمكن أن يكون لهذه المعايير عقوبات صارمة إذا كان الإهمال يؤدي إلى اختراق بيانات التعريف الشخصية. وتنظر شركات الأمن السيبراني في كيفية جمع البيانات وتخزينها ونقلها، من خلال وضع وسائل حماية لضمان تشفير البيانات حسب الحاجة لحمايتها من التسلل.

ت- التخطيط للتعافي من الكوارث:

تسعى العديد من الشركات للحصول على المساعدة من خدمات استشارات الأمن السيبراني عندما يتعلق الأمر بتخطيط التعافي من الأزمات هذا هو المفتاح للحفاظ على العمل وتشتمل حماية التعافي من الكوارث على مكونين مهمين:

- استراتيجيات لمنع وقوع اختراق أو إصابة بالبرامج الضارة.

- الاستعدادات للشفاء السريع في حالة وقوع ضحية لهجوم.

ج- أمن الشبكة:

ويعني ممارسة تأمين شبكة الكمبيوتر من المتطفلين، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية. ويتضمن أمن الشبكة حماية شبكتك المادية وجميع الأجهزة المتصلة بها. وتستخدم معظم الشركات جدران الحماية لمراقبة حركة المرور الواردة والصادرة بحثاً عن التهديدات. ويعد تأمين الشبكات اللاسلكية والتأكد من حدوث أي اتصالات عن بعد من خلال طرق مشفرة من الطرق التي تتضمن بها خدمات الأمن السيبراني أمن الشبكة.

ح- أمن المستخدم النهائي:

ويعرف أمن المستخدم النهائي أيضاً باسم أمن نقطة النهاية، ويشير هذا إلى حماية الأجهزة التي يعمل بها المستخدمون أنفسهم. ويعد أمن المستخدم النهائي أمراً حيوياً، نظراً لأن 91% من الهجمات الإلكترونية تبدأ برسالة بريد إلكتروني للتصيد الاحتيالي. وتتضمن بعض الأنواع الأكثر شيوعاً لحماية المستخدم النهائي التي يجب أن تتمتع بها ما يلي:

- تحديث الأجهزة باستمرار.

-إدارة مكافحة الفيروسات / مكافحة البرامج الضارة.

-تصفية DNS لحظر المواقع الضارة.

-حماية البرامج الثابتة لمنع الخروقات في طبقة البرامج الثابتة.

د- الأمن التشغيلي:

ويعني العمليات والقرارات الخاصة بمعالجة أصول البيانات وحمايتها، والأذونات التي يمتلكها المستخدمون عند الوصول إلى شبكة والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها كلها تندرج تحت هذه المظلة. ويتضمن الأمن التشغيلي اتخاذ خطوة إلى الوراء والنظر إلى استراتيجيتك الأمنية بالكامل للتأكد من أن جميع التكتيكات الأمنية تعمل في انسجام خلال عملياتك، وعدم تعارض أي منها مع بعضها البعض¹.

-2أبرز التهديدات الرقمية :

•البرامج الضارة (Malicious Codes) يتسم هذا التهديد بأنه من أشهر المخاطر التي تهدد الأمن السيبراني خاصة والانترنت عامة إذ تتسلل البرامج للأنظمة وتثبت نفسها على النظام بهدف الوصول غير المصرح به للملفات وإلحاق الأذى بها أو سرقتها

•سرقة كلمة المرور (Passwords penetration) تلاحظ بمجرد محاولة الولوج للحساب، إذ يتبين وجود تغيير في كلمة المرور، وهذا مؤشر على أن شخصاً ما تمكن من اختراق النظام والحصول على البيانات السرية.

•التنصت (Eavesdrop on data) يتمثل في قدرة أحد الأطراف على مراقبة البيانات المنتقلة بين المستخدم والمضيف، وهذا يعني سرقة المعلومات من النظام بناءً على حركة التنصت المطبقة.

•هجمات التصيد (Data phishing attacks) تكون عبر رسائل رسمية من جهات رسمية تطلب كلمات المرور أو بيانات هامة، وهنا يقع المستخدم في خطأ تقديم بياناته للمتصيدين من خلال الضغط على روابط مشبوهة مثلاً.

•رفض الخدمة الموزع (DDoS) يستهدف هذا الخطر الخوادم الرئيسية في هذه الحالات يقوم الخادم بتوقيف موقع الويب التي تحاول الوصول للبيانات أو يحدث بطء في أداء الخوادم.

•هجوم عبر الموقع (Cross-site attack on data) يتم عبر استهداف المواقع الضعيفة وتحميل رموز خطيرة عليها، مما يعرض بيانات المستخدمين للسرقة أو التسبب في عطل الخدمات الرئيسية لها .

¹ سناء أحمد عبد الله الشديفات، "الأمن السيبراني وحماية البيانات والمعلومات في أقسام بلدية منشية بني حسن"، مجلة العلوم الإنسانية والطبيعية(HNSJ) ، المجلد 5، العدد 1 (2024): 8-816

- هجوم SQL: يُعد هذا الهجوم برنامجاً لمعالجة البيانات، بحيث يتيح للأطراف الخارجية الوصول للمعلومات غير المتاحة، والمعلومات الحساسة من خلال عدد من البرمجيات.
- برامج الفدية: Ransomware تثبت عدد من البرامج الضارة على الأنظمة، مما يؤدي إلى منع الوصول إلى النظام، وبالتالي يطالب الطرف الخارجي من المستخدم دفع فدية مقابل إزالة هذه البرامج.
- فيروس طروادة: Trojan Horse يُمكن دخول للنظام من خلال برامج تنتزه برامج قانونية من خلال التنبيهات التي تُظهر للمستخدم حاجة النظام الخاص به للمسح الضوئي، وهنا تستطيع البرامج الضارة الدخول للنظام من خلال عملية المسح¹.

المطلب الثالث: أهمية وأهداف الأمن السيبراني وشروط تحقيقه

في ظل التوسع الرقمي الحالي، صار الأمن السيبراني موضوعاً في غاية الأهمية لحماية البيانات والمعلومات الحساسة ومع تزايد التهديدات السيبرانية باستمرار، أصبح فهم المبادئ والممارسات الأساسية للأمن السيبراني أمراً ضرورياً جداً لضمان سلامة المعلومات والحفاظ على خصوصية الأفراد والمؤسسات على حد سواء².

1- أهمية الأمن السيبراني:

لقد جعل تزايد الرقمنة في جميع القطاعات البيانات من أهم الأصول لأي مؤسسة حيث يؤدي فقدان المعلومات الحساسة ليس فقط إلى خسائر مالية كبيرة، بل أيضاً إلى فقدان ثقة العملاء والتعرض للمساءلة القانونية وفي أسوأ الأحوال قد تصل إلى إغلاق المؤسسة.

علاوة على ذلك، لا يقتصر الأمن السيبراني في هندسة الأنظمة على حماية معلومات العملاء أو الشركات فحسب، بل يشمل أيضاً حماية البنية التحتية الحيوية مثل أنظمة التحكم الصناعية الحيوية لتشغيل الخدمات الأساسية كالمياه والطاقة والرعاية الصحية وقد يُسفر أي هجوم على هذه الأنظمة عواقب وخيمة مما يستوجب حلول فعالة ومن المهم التأكيد على أن غياب الأمن السيبراني الجيد يُمكن أن يؤثر سلباً على النظام البيئي بأكمله فالجميع عرضة للهجمات لذلك يُعد تعزيز ثقافة الأمن السيبراني في جميع مراحل تطوير البرمجيات أمراً بالغ الأهمية ويجب اعتباره استثماراً لا نفقة³.

2- أهداف الأمن السيبراني:

تهدف جهود الأمن السيبراني إلى ضمان سلامة المعلومات. ويمكن تلخيص أبرز هذه الأهداف في الآتي:

¹ أبرز التهديدات الرقمية"، المجلة الدولية للعلوم والتقنية (ISTJ)، العدد 29 (أبريل 2022)، ص. 10-11.

² علاء عبد الخالق حسين وآخرون، مرجع سابق ص. 9

³ رمضان مراد، التنقيف والتوعية بالأمن السيبراني (وهران: دار العيون للنشر الإلكتروني، 2025)، ص. 5.

- الحفاظ على دقة وسلامة البيانات والبرامج وعدم فساد حالتها.
- الحفاظ على البيانات والبرامج للفترة المطلوبة.
- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
- التصدي للهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاعين العام والخاص.
- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- صمود البنى التحتية الحساسة للهجمات الإلكترونية.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- التخلص من نقاط الضعف في أنظمة أمن الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
- سد الثغرات في أنظمة أمن المعلومات.
- مقاومة البرمجيات الخبيثة.
- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة¹.

وبهذا، تسعى أهداف الأمن السيبراني إلى الحفاظ على المعلومات وسلامتها عبر منع العبث بها، وضمان جاهزيتها عند الحاجة إليها، وحماية الأجهزة والشبكات لتكون درعاً واقياً للبيانات بالإضافة إلى استكشاف الثغرات في الأنظمة ومعالجتها كما تهدف إلى استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني، وتوفير بيئة عمل آمنة عبر الشبكة العنكبوتية².

3- شروط تحقيق الأمن السيبراني:

لضمان بيئة رقمية آمنة وحماية البيانات من مختلف التهديدات، هناك مجموعة من الشروط الضرورية التي يجب توفرها، والتي يختصرها المختصون في نموذج (CIA)، وهي تشمل السرية، السلامة، والتوفر، وهي كما يلي:

¹ منى عبد الله السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، العدد 11 (جولية 2020): 12.

² أماني محمد شريف وآخرون، "بروفيلات الانفعالات المرتبطة بالتحصيل المتميزة"، المجلة العلمية لكلية التربية - جامعة أسيوط، المجلد 40، العدد 11 (2024): 159.

1- السرية: تعد السرية أو الخصوصية من أبرز الشروط؛ حيث يجب على سياسات الشركة تقييد الوصول إلى المعلومات بالنسبة إلى الموظفين المصرح لهم والتأكد من أن الأفراد المصرح لهم فقط هم من يشاهدون هذه البيانات. قد تتم تجزئة البيانات وفقاً لمستوى الأمان أو مستوى حساسية المعلومات على سبيل المثال، لا يجب على مطوري برامج Java الوصول إلى المعلومات الشخصية لجميع الموظفين علاوة على ذلك، يجب على الموظفين تلقي التدريب لفهم أفضل الممارسات في حماية المعلومات الحساسة لحماية أنفسهم والشركة من الهجمات. يتضمن طرق ضمان السرية تشفير البيانات، ومعرفة اسم المستخدم وكلمة المرور، والمصادقة الثنائية، وتقليل تعرض المعلومات الحساسة للخطر.

2- السلامة: تعتبر السلامة هي دقة واتساق وموثوقية البيانات خلال دورة حياتها بالكامل، حيث يجب أن تظل البيانات دون تغيير أثناء النقل ولا تتغير بواسطة كيانات غير مصرح بها. كما يمكن استخدام التحكم في الإصدار لمنع التغييرات غير المقصودة بواسطة المستخدمين المصرح لهم أيضاً. يجب أن تكون النسخ الاحتياطية متوفرة لاستعادة أي بيانات تالفة ويمكن استخدام تجزئة المجموع الاختباري للتحقق من تكامل البيانات أثناء النقل.

3- التوفر: الحفاظ على المعدات، وإجراء إصلاحات الأجهزة، والحفاظ على تحديث أنظمة التشغيل والبرامج، وإنشاء نسخ احتياطية تضمن توفر الشبكة والبيانات المستخدمين المعتمدين. يجب أن تكون الخطط جاهزة للتعافي بسرعة من الكوارث الطبيعية أو الكوارث التي من صنع الإنسان. المعدات أو البرامج الأمنية، مثل الجدران النارية، تحميكم من التوقف بسبب هجمات مثل حجب الخدمة (DoS) يحدث حجب الخدمة عندما يحاول أحد المهاجمين إرباك الموارد بحيث لا تتوفر الخدمات للمستخدمين¹.

المطلب الرابع: النظريات المفسرة للأمن السيبراني

تظهر أهمية النظريات الأساسية في الأمن السيبراني في توجيه الاستراتيجيات لحماية المعلومات والبيانات الحساسة. حيث تُظهر الأبحاث أن فهم النظريات السيبرانية يمكن أن يزيد من قدرة المؤسسات على التكيف مع التهديدات المتزايدة في العالم الرقمي و مع تقدم التكنولوجيا، ظهرت تحديات جديدة تحتاج لنموذج مرنة لإدارة المخاطر.

وتوجد جملة من نظريات الأنظمة المعلوماتية التي يمكن تطبيقها في مجال الأمن السيبراني بقصد فهم وتفسير الظاهرة ومن بين هذه النظريات نجد:

¹ Cisco Networking Academy, Introduction to Cyber Security Course (2021), 17–19.

1- نظرية السلوك المخطط :

تشير هذه النظرية إلى أنه من الضروري على المؤسسات تطبيق وتوفير إجراءات أمنية قوية للحد من الهجمات السيبرانية سواء على نظامها المعلوماتي أو موردتها البشري، إذ أن غيابها يشكل خطراً على البنية الرقمية والمعلوماتية للمؤسسة ويشكل هذا تهديداً للعنصر البشري بشكل مباشر أو غير مباشر من أبرز مخرجات الاساسية لهذه النظرية:

• أ- التحول الرقمي الذي عرفته المؤسسات نتيجة التطور التكنولوجي يفرض عليها الاعتماد على أنظمة الحماية السيبرانية عبر استخدام جدران الحماية وبرامج مكافحة الفيروسات والنسخ الاحتياطي للبيانات مع التحكم في صلاحيات الوصول لقواعد البيانات بالنسبة للعمال وإلزامهم باتباع كافة الخطوات الأمنية قبل الولوج لواجهة العمل لضمان حمايتهم.

ب- اتباع سياسة للأمن السيبراني تعتمد على التطوير التقني وبرامج متطورة لحماية البنية الرقمية مع التركيز على تدريب وتوعية الموظف فكلما زاد مستوى الإدراك للمخاطر السيبرانية التي تواجهه عند استخدام الإنترنت أثناء العمل كلما كانت نسبة وقوع الخطر قليلة.

ت- دراسة العوامل المؤثرة على الموظفين تساهم في بناء المخطط الأمني الذي تدير عليه المؤسسة في سياستها الامنية لأن ضبط هذه العوامل هو الركيزة الأهم في تحليل وتفسير مشاكل التفاعل داخل التنظيم بالإضافة إلى أهمية الحوار المتبادل بين الأعضاء بشأن سياسات الأمان الواجب اتباعها باعتبار أن الموظف غالباً ما يمثل الحلقة الأضعف¹.

2- نظرية الردع:

ترى هذه النظرية إلى أن السلوك البشري المرتبط بالأنشطة غير مشروعة يمكن السيطرة عليه في حال وجود عقوبات صارمة وقد قدمت نظرية الردع عدة افتراضات لتفسير هذه الظاهرة منها:

أ- يبقى المورد البشري هو الحلقة الضعيفة في استغلال النظام وسوء تسييره مما يتسبب في اختلال الأمن الداخلي للمؤسسة.

ب- ترتبط أغلب حوادث الكومبيوتر بالأعمال الداخلية للمستخدمين المرخص لهم وبالرغم من التطور الكبير في رصد ومنع الهجمات الخارجية إلا أنه لا توجد حماية مطلقة ضد هذه الثغرات الرقمية.

¹ عبد الرزاق برادة، "مستوى الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية" (أطروحة دكتوراه غير منشورة، جامعة غليزان، الجزائر، 2024) ص15.

ت- يؤدي استغلال النظام المعلوماتي على الرغم من وجود إجراءات أمنية فعالة بسبب سوء السلوك البشري الذي يعتبر من التهديدات الداخلية للمؤسسة سواء كان ذلك بشكل متعمد أو عن طريق الخطأ.

-3- نظرية حماية التحفيز:

ترى نظرية التحفيز ان المؤسسات تواجه العديد من المشكلات الأمنية بسبب عدم التزام الموظفين بسياسات الأمن الداخلي وهذا راجع كونهم يفكرون في احتمال اتخاذ إجراءات (الكفاءة الذاتية) وما إذا كانت هذه الإجراءات ستؤدي إلى نتائج مرغوبة محددة (الاستجابة). وقد قدمت نظرية حماية التحفيز عدة افتراضات لتفسير هذه الظاهرة منها:

أ- ترى أن المؤسسة بحاجة إلى ضمان عدم تعرض أنظمة الكمبيوتر والبنية الرقمية ومعلوماتها للخطر.

ب- اتخاذ التدابير الأمنية المناسبة في مكانها.

ت- يستوجب التزام الموظفين بسياسة الأمنية داخل المؤسسة¹.

المبحث الثاني : الوعي بالأمن السيبراني في الوسط الجامعي

جاء التقدم التكنولوجي مصحوباً بصور مستحدثة من التحديات الرقمية التي تستعير من هذه التقنية أساليبها المتطورة فأصبحنا أمام ظاهرة جديدة هي ظاهرة الجريمة المعلوماتية ، مما جعل معظم الدول تهتم بتطوير الأمن السيبراني للتخفيف من مخاطر اختراق المعلومات والهجمات الإلكترونية التي تتطلب تعزيز الوعي السيبراني بين مختلف فئات المجتمع حيث أصبح الأمن السيبراني هو الوسيلة الوحيدة للحفاظ على سرية المعلومات الخاصة بالأفراد والمؤسسات².

المطلب الأول : تعريف الوعي السيبراني

يمكن النظر إلى الوعي السيبراني على أنه مستوى التقدير أو الفهم أو المعرفة بجوانب الأمن السيبراني أو أمن المعلومات وتشمل هذه الجوانب الإدراك بالمخاطر والتهديدات السيبرانية وأيضاً تدابير الحماية المناسبة³.

¹ المرجع نفسه ، ص 16.

² الحسيني فايزة، "الوعي بالأمن السيبراني: ترف أم ضرورة في عصر المعلومات"، مجلة Educ Recherche ، المجلد 13، العدد 2 (2023): ص 54 .

³ Jason R. C. Nurse, "Cybersecurity Awareness," University of Kent, UK, published June 30, 2022

كما يُعدّ الوعي بالأمن السيبراني عملية مستمرة لتثقيف وتدريب الأفراد حول المخاطر الكامنة في الفضاء الإلكتروني، وكيفية الوقاية منها وما يجب عليهم فعله في حال وقوع حادث أمني كما يُساهم ذلك في غرس شعور بالمسؤولية الاستباقية لديهم تجاه الحفاظ على سلامة الأصول الرقمية .

وببساطة، يعني الوعي بالأمن السيبراني معرفة ماهية المخاطر الأمنية والتصرف بمسؤولية لتجنب المخاطر المحتملة؛ ويشمل الإلمام بأحدث التهديدات الأمنية وأفضل الممارسات في هذا المجال، ومخاطر النقر على روابط خبيثة أو تحميل مرفقات مصابة والتفاعل عبر الإنترنت والإفصاح عن معلومات حساسة¹.

كما يشير الوعي بالأمن السيبراني إلى مدى توعية الأفراد والمؤسسات بمخاطر الأمن السيبراني والتحديات التي تنطوي عليها والقدرة على فهم كيفية حماية الأنظمة والبيانات الرقمية².

وعليه، يمكن القول إن عالم اليوم يسير بخطى سريعة وأن التكنولوجيا وكذلك الهجمات السيبرانية تتطور باستمرار حيث إن أساليب الوعي بالأمن السيبراني غالباً ما تكون ثابتة ولا تتلاءم مع مشهد التهديدات المتغير هذا أو الطبيعة الابتكارية لمجرمي الإنترنت لذا يلزم إجراء بحث في أطر ومنصات تكيفية للوعي بالأمن السيبراني تكون مرنة ويمكن تحديثها بسرعة، لضمان حصول المستخدمين على فرصة لحماية أنفسهم ضد المهاجمين.

المطلب الثاني: أهمية الوعي بالأمن السيبراني في الجامعات

أصبحت الجامعات في العصر الرقمي تعتمد بشكل متزايد على التقنيات الإلكترونية في مختلف تفاصيلها الأكاديمية والإدارية، مما جعل الوعي بالأمن السيبراني عنصراً أساسياً في حماية الأنظمة والمعلومات وفي هذا السياق، تبرز الثقافة السيبرانية بوصفها أحد أهم ركائز الوعي الرقمي حيث لا تقتصر على الجوانب التقنية فحسب بل تشمل السلوكيات الواعية والممارسات الصحيحة في استخدام التكنولوجيا ، وتمثل شريحة الطلبة النسبة الأكبر من مستخدمي الأنظمة الجامعية مثل المنصات التعليمية والبريد الإلكتروني وأنظمة معلومات الطلبة، الأمر الذي يجعل وعيهم الأمني عاملاً حاسماً في تقليل المخاطر السيبرانية فالسلوكيات غير الآمنة كاستخدام كلمات مرور ضعيفة أو التعامل غير الحذر مع الروابط والملفات قد تشكل مدخلاً للهجمات الإلكترونية التي تهدد وعي الجامعة بأكملها فيساهم الطلبة في تعزيز الثقافة السيبرانية من خلال التزامهم بالممارسات الرقمية الآمنة مثل حماية بياناتهم الشخصية واحترام سياسات استخدام الأنظمة والإبلاغ عن أي نشاط مشبوه كما تلعب

¹ موقع Kaseya ، "الوعي بالأمن السيبراني: التعريف والأهمية والغرض والتحديات"، نشر في 30 يونيو 2022، تاريخ الاطلاع 12 مايو 2026، متاح على الرابط <https://www.kaseya.com> :

² عمرو نعوم، "الوعي بالأمن السيبراني: ما هو ولماذا يهم؟"، موقع Root-X ، نشر في 24 سبتمبر 2023، تاريخ الاطلاع 12 مايو 2026، متاح على الرابط <https://root-x.com> :

مشاركتهم في الدورات التدريبية وورش العمل التوعوية دوراً مهماً في رفع مستوى الوعي الجماعي وتعزيز الفهم العملي لمخاطر الفضاء السيبراني كما تُعد الأنشطة الطلابية العلمية مثل الندوات والمسابقات والمبادرات التطوعية من الوسائل الفعالة لنشر الثقافة السيبرانية داخل الجامعات إذ تتيح هذه الأنشطة للطلبة تبادل المعرفة والخبرات والمساهمة في بناء بيئة جامعية أكثر أماناً من خلال العمل الجماعي والتفاعل الإيجابي¹.

وبهذا فإن تعزيز الثقافة السيبرانية داخل الجامعات من خلال الطلبة ينعكس إيجاباً على المجتمع ككل حيث يُساهم في إعداد جيل واعٍ بأهمية الوعي الرقمي وقادر على استخدام التكنولوجيا بشكل مسؤول ويؤكد ذلك أن الطلبة ليسوا مجرد متلقين للمعرفة بل شركاء فاعلين في بناء منظومة وعي سيبراني مستدامة داخل المؤسسات التعليمية².

المطلب الثالث: دور الجامعات في تعزيز الوعي بالأمن السيبراني

يبرز دور الجامعات في دعم الطلبة وتمكينهم من أداء هذا الدور، عبر دمج مفاهيم الأمن السيبراني في المناهج الدراسية، وتشجيع البحث العلمي الطلابي في هذا المجال، فضلاً عن توفير بيئة تعليمية تحفز على الابتكار والمسؤولية الرقمية. ويسهم هذا الدعم في إعداد طلبة قادرين على مواجهة التحديات السيبرانية داخل الجامعة وخارجها. إن تعزيز الثقافة السيبرانية داخل الجامعات من خلال الطلبة ينعكس إيجاباً على المجتمع ككل، حيث يُساهم في إعداد جيل واعٍ بأهمية الأمن الرقمي وقادر على استخدام التكنولوجيا بشكل مسؤول. ويؤكد ذلك أن الطلبة ليسوا مجرد متلقين للمعرفة، بل شركاء فاعلين في بناء منظومة أمن سيبراني مستدامة داخل المؤسسات التعليمية.

حيث تعد الجامعات مهمة في بناء الوعي الرقمي وزيادة الكفاءات في المجتمع، فهي تعتمد استراتيجيات تعليمية تركز على الأمن السيبراني كجزء أساسي من المناهج. عبر برامج دراسات متخصصة، تسعى الجامعات لتجهيز الطلاب بالمعرفة والمهارات اللازمة لمواجهة التهديدات المتزايدة في الفضاء السيبراني. هذه البرامج لا تتعلق فقط بالتعلم النظري، بل تشمل أيضاً تجارب عملية مثل ورش العمل والتدريب العملي، مما يقوي قدرة الطلاب على الإسهام الفعال في مؤسساتهم المستقبلية. كما تساعد هذه المبادرات في خلق بيئة تعليمية تدعم التفكير النقدي والتحليلي، مما يسهل الاستجابة للتحديات المختلفة في مجال الأمن السيبراني كما تواجه المؤسسات التعليمية تحديات كثيرة في تحقيق هذا الهدف، مثل قلة الوعي بأهمية الأمن السيبراني بين بعض الفئات. لذلك، ينبغي على

¹ علي حسن بدر المعيد، "دور الطلبة في تعزيز الثقافة السيبرانية داخل الجامعات"، كلية العلوم، قسم الأمن السيبراني، جامعة المستقبل (العراق)، نُشر في 6 فبراير 2026، تاريخ الاطلاع 12 ماي 2026، متاح على الرابط

<https://uomus.edu.iq>.

² المرجع نفسه.

الجامعات وضع سياسات واضحة لضمان إدماج الأمن السيبراني في جميع مجالات الدراسة، وتقديم ورش عمل تدريبية للمعلمين، مما يعزز من قدرتهم على تدريس مفاهيم الأمن الرقمي بنحو فعال. علاوة على ذلك، يمكن أن تؤدي الجامعات دوراً قيادياً عن طريق التعاون مع الجهات الحكومية والقطاع الخاص، حيث يتم تبادل المعرفة والخبرات. هذه الشراكات ستساعد في تطوير برامج تعليمية شاملة تتناسب مع التطورات في الأمن السيبراني وتلبي احتياجات سوق العمل المتغيرة. أيضاً، ينبغي على الجامعات أن تسعى لتطوير برامج توعوية وإعلامية تستهدف المجتمع المحلي، لزيادة الوعي الرقمي خارج الحرم الجامعي. يمكن استخدام وسائل التواصل الاجتماعي والبرامج التفاعلية لجذب الشباب وتعليمهم بالمخاطر السيبرانية وطرائق الوقاية منها. من خلال هذه الجهود، ستسهم الجامعات في بناء مجتمع رقمي مستنير يقاوم التهديدات الأمنية بنحو كبير¹.

المطلب الرابع: استراتيجيات تعزيز الوعي السيبراني في الوسط الجامعي

مع تزايد الهجمات السيبرانية على المؤسسات التعليمية، أصبح من الضروري تبني استراتيجيات فعالة لتعزيز الأمن السيبراني إذ تهدف هذه الاستراتيجيات إلى حماية البيانات وتأمين الأنظمة وتعزيز الوعي الأمني لدى جميع أفراد المجتمع الأكاديمي ومن بين أهم هذه الاستراتيجيات: تطوير سياسات وإجراءات أمنية شاملة تدريب الكوادر التعليمية والإدارية استخدام تقنيات حديثة وتعزيز التعاون مع الجهات المختصة².

1- تطوير سياسات وإجراءات أمنية شاملة:

يُعد تطوير سياسات أمنية واضحة ومحددة من الركائز الأساسية للأمن السيبراني في المؤسسات التعليمية حيث تضع هذه السياسات القواعد والإرشادات التي تحدد كيفية التعامل مع البيانات، واستخدام الأنظمة والاستجابة للحوادث الأمنية كما أن وجود سياسة واضحة يساعد على تقليل الأخطاء البشرية التي قد تؤدي إلى اختراقات أمنية، إذ تشير الأبحاث إلى أن 90% من الحوادث السيبرانية ناتجة عن أخطاء بشرية أو ضعف في الامتثال للإجراءات الأمنية. بالإضافة إلى ذلك، يجب تحديث السياسات الأمنية بشكل مستمر لمواكبة التهديدات المتطورة، حيث أظهرت دراسة حديثة أن المؤسسات التي تقوم بتحديث سياساتها الأمنية بانتظام تكون أقل عرضة للهجمات السيبرانية بنسبة 30% مقارنة بالمؤسسات التي تعتمد على سياسات قديمة.

¹ علاء عبد الخالق حسين وآخرون، مرجع سابق، 35.

² M. Aljumaily, Strategies for Enhancing Cybersecurity and Data Protection in Arabic Educational Institutions in Light of Digital Transformation (2025), 6-8.

-2- تدريب الكوادر التعليمية والإدارية :

يُعد تدريب الموظفين وأعضاء هيئة التدريس والطلاب على الأمن السيبراني من أهم الخطوات لتعزيز الحماية الإلكترونية؛ فالتوعية المستمرة والتدريب على كيفية التعرف على الهجمات الإلكترونية، مثل التصيد الاحتيالي، يقلل من فرص نجاح هذه الهجمات.

-3- استخدام تقنيات حديثة :

تلعب التقنيات الحديثة دوراً حاسماً في تعزيز الأمن السيبراني، ومن أبرزها:

• تطبيق التشفير لحماية البيانات: يُعتبر التشفير من أهم الوسائل لحماية البيانات الحساسة من الوصول غير المصرح به؛ فعلى سبيل المثال، تستخدم العديد من الجامعات تشفير البيانات عند تخزينها أو نقلها عبر الشبكات لضمان عدم تعرضها للسرقة أو التلاعب.

• المصادقة متعددة العوامل (MFA): تساعد في تقليل فرص الاختراق من خلال إضافة طبقات حماية إضافية عند تسجيل الدخول إلى الأنظمة؛ إذ أظهرت دراسة أن استخدام (MFA) يقلل من احتمالية سرقة الحسابات بنسبة 99.9% مقارنة بالاعتماد على كلمات المرور وحدها.

-4- تعزيز التعاون مع الجهات المختصة :

إن تعزيز الأمن السيبراني في المؤسسات التعليمية لا يمكن تحقيقه دون التعاون مع الجهات المختصة، مثل شركات الأمن السيبراني، والمؤسسات الحكومية المعنية بحماية البيانات¹.

¹ مرجع نفسه ص 8.

خلاصة:

من خلال ما تقدم يتضح أن دراسة الأمن السيبراني والوعي به تستند إلى إطار نظري ومفاهيمي متعدد الأبعاد. فمن جهة، يتطلب الأمر فهماً عميقاً للأمن السيبراني كاستراتيجية دفاعية لا غنى عنها في ظل التهديدات الرقمية المتزايدة وفهم خصائص هذا المجال وعناصره وأبرز تهديداته الرقمية، مع الإقرار بضرورة توفر شروط الحماية (السرية، السلامة، التوفر).

ومن جهة أخرى، تستدعي الدراسة الاطلاع على المفاهيم الأساسية للوعي بالأمن السيبراني وأهميته في الوسط الجامعي كما يبرز دور الجامعة كركيزة أساسية في تعزيز هذا الوعي عبر استراتيجيات تعليمية وتدريبية مع الإقرار بالتحديات التي تواجه المؤسسات التعليمية في هذا المجال.

الفصل الثالث

الإطار التطبيقي

تمهيد:

يُشكل هذا الفصل المحطة العملية التي تُترجم فيها الإطار النظري للدراسة إلى واقع ملموس، حيث نسعى من خلاله إلى اختبار الفرضيات التي تم طرحها مسبقاً وتفكيك متغيراتها عبر تحليل ميداني دقيق فالانتقال من سياق المفاهيم والتعريفات إلى سياق الممارسة البحثية يُعد ركيزة أساسية لتعزيز مصداقية النتائج إذ يسمح لنا بملامسة اتجاهات عينة الدراسة بشكل مباشر وتحويل استجاباتهم إلى مؤشرات رقمية وتحليلية ذات دلالة علمية.

يتناول هذا الفصل بالدراسة والتحليل واقع "الأمن السيبراني لدى طلبة الإعلام الآلي بجامعة محمد بوضياف بالمسيلة"، حيث نعتمد على استمارة الاستبيان كأداة رئيسية لجمع البيانات موزعة على محاور خمسة مترابطة نبدأ فيها باستعراض الخلفية المعرفية للطلبة حول الأمن السيبراني مروراً بتقييم الدور الجامعي في هذا المجال وصولاً إلى فحص الممارسات الرقمية اليومية للطلبة واستشراف إدراكهم للمخاطر المحيطة بهم وانتهاءً برصد مقترحاتهم العملية لتطوير مستوى الحماية الرقمية داخل الوسط الأكاديمي.

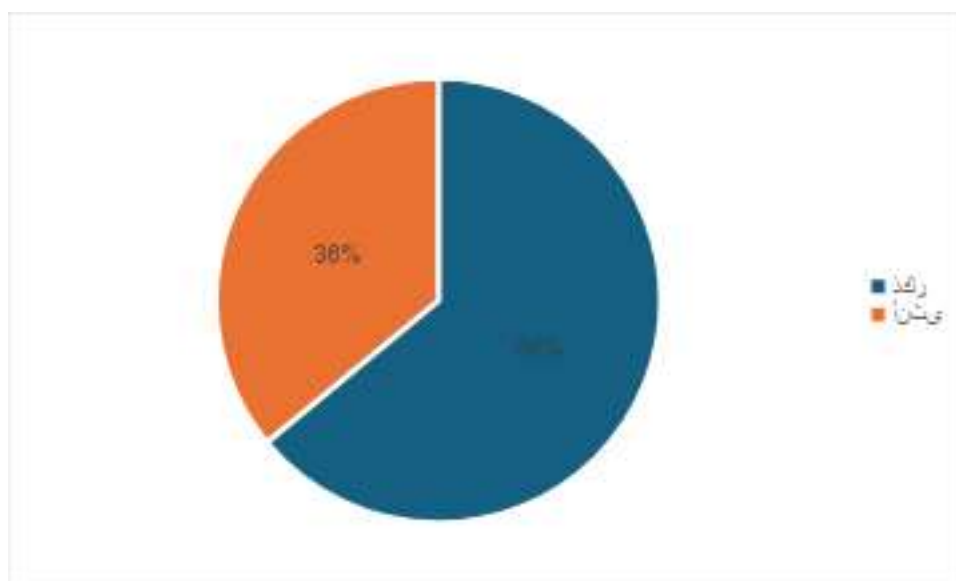
عرض وتحليل النتائج

أ/ تحليل البيانات الوصفية:

الجدول رقم (01) يوضح توزيع أفراد عينة الدراسة حسب متغير الجنس

الجنس	التكرارات	النسبة المئوية
ذكر	32	64%
أنثى	18	36%
الإجمالي	50	100%

من خلال الجدول أعلاه وبالنظر إلى تكرارات أفراد عينة الدراسة والبالغ حجمهم إجمالاً 50 فرداً، نلاحظ أن 32 فرداً يمثلون حجم الذكور بنسبة بلغت 64%، أما حجم الإناث فقد بلغ 18 بنسبة قدرت بـ 36%، وهذا ما هو موضح من خلال التالي:

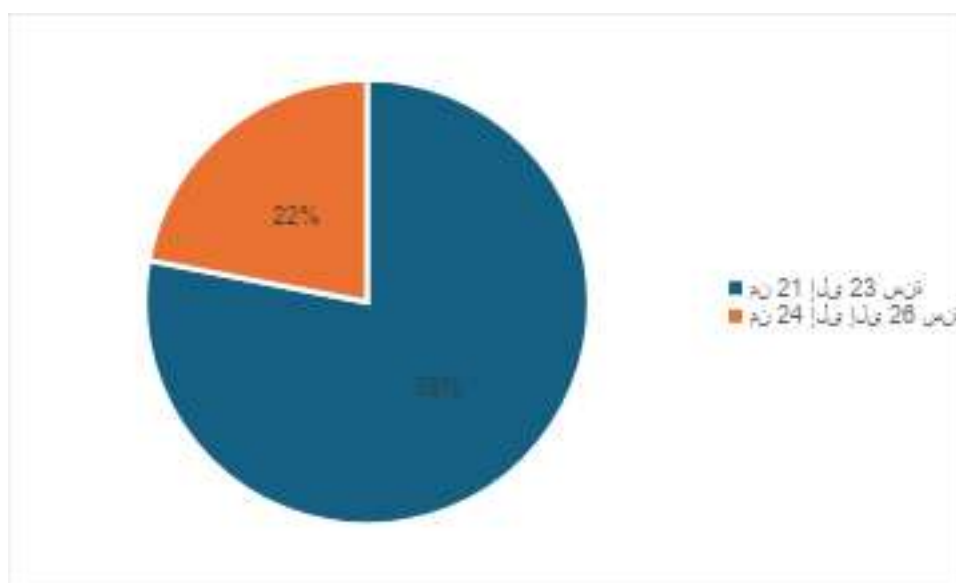


الشكل رقم (01) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير الجنس

الجدول رقم (02) يوضح توزيع أفراد عينة الدراسة حسب متغير السن

السن	التكرارات	النسبة المئوية
من 21 إلى 23 سنة	39	78%
من 24 إلى 26 سنة	11	22%
الإجمالي	50	100%

من خلال الجدول أعلاه وبالنظر إلى تكرارات أفراد عينة الدراسة والبالغ حجمهم إجمالاً 50 فرداً، نلاحظ أن 39 فرداً يمثلون الفئة العمرية (من 21 إلى 23 سنة) بنسبة بلغت 78%، أما الفئة العمرية (من 24 إلى 26 سنة) فقد بلغ حجمها 11 فرداً بنسبة قدرت بـ 22%، وهذا ما هو موضح من خلال الشكل التالي:

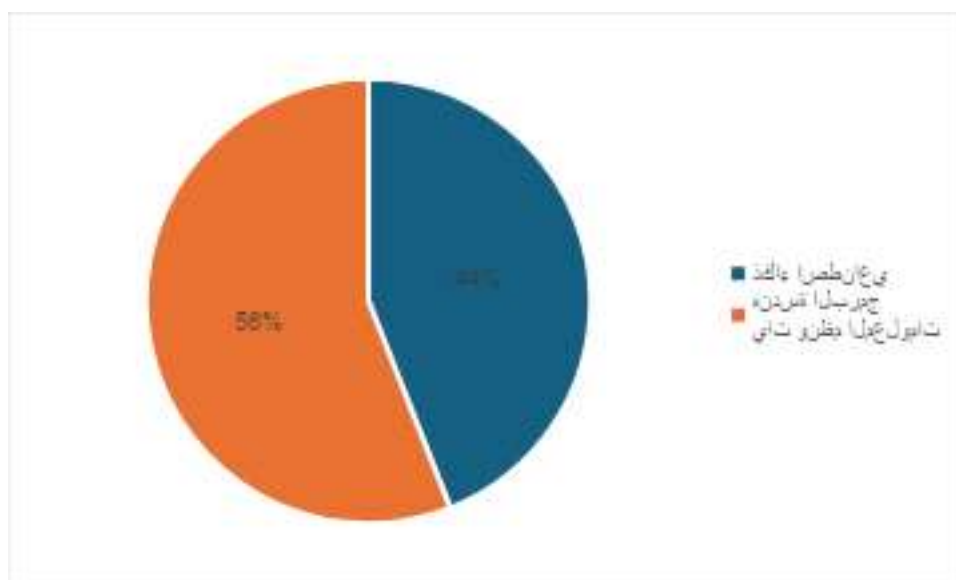


الشكل رقم (02) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير السن

الجدول رقم (03) يوضح توزيع أفراد عينة الدراسة حسب متغير التخصص

التخصص	التكرارات	النسبة المئوية
ذكاء اصطناعي	22	44%
هندسة البرمجيات ونظم المعلومات	28	56%
الإجمالي	50	100%

من خلال الجدول أعلاه وبالنظر إلى تكرارات أفراد عينة الدراسة والبالغ حجمهم إجمالاً 50 فرداً، نلاحظ أن 22 فرداً يمثلون تخصص (ذكاء اصطناعي) بنسبة بلغت 44%، أما تخصص (هندسة البرمجيات ونظم المعلومات) فقد بلغ حجمهم 28 فرداً بنسبة قدرت بـ 56%، وهذا ما هو موضح من خلال الشكل التالي:

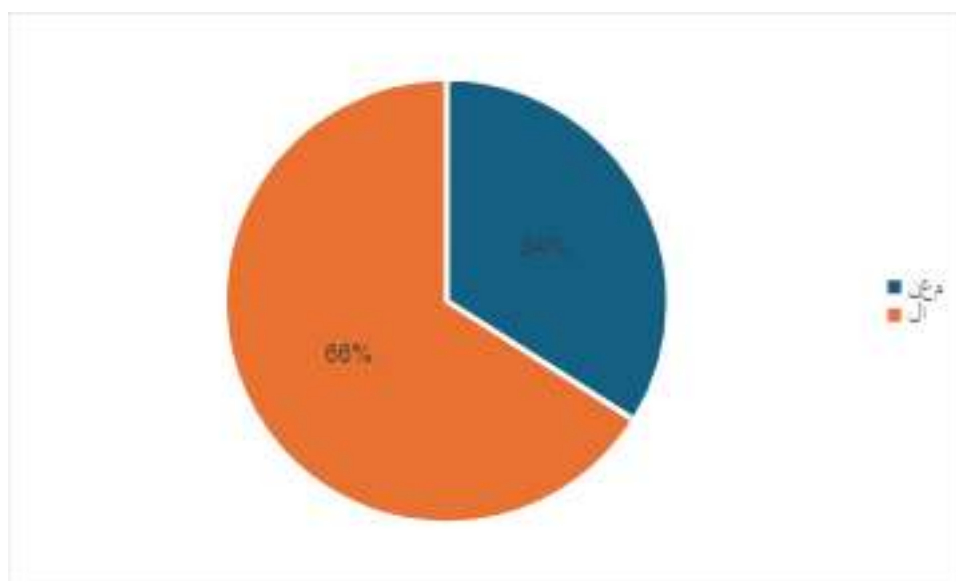


الشكل رقم (03) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير التخصص

الجدول رقم (04) يوضح توزيع أفراد عينة الدراسة حسب متغير التعرض للاختراق

التعرض للاختراق	التكرارات	النسبة المئوية
نعم	17	34%
لا	33	66%
الإجمالي	50	100%

من خلال الجدول أعلاه وبالنظر إلى تكرارات أفراد عينة الدراسة والبالغ حجمهم إجمالاً 50 فرداً، نلاحظ أن 17 فرداً يمثلون فئة الذين سبق لهم التعرض للاختراق بنسبة بلغت 34%، أما الذين لم يسبق لهم التعرض للاختراق فقد بلغ حجمهم 33 فرداً بنسبة قدرت بـ 66%، وهذا ما هو موضح من خلال الشكل التالي:



الشكل رقم (04) يوضح توزيع نسب أفراد عينة الدراسة حسب متغير التعرض للاختراق

ب/ تحليل أسئلة الاستبيان:

أولاً/ الجداول البسيطة

المحور الأول: مستوى المعرفة بالأمن السيبراني

البند رقم (01):

نص البند رقم (01) على: " لدي معرفة ببعض المفاهيم الأساسية للأمن السيبراني، مثل التشفير وحماية البيانات". وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (05) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (01)

البديل	التكرارات	النسبة المئوية
موافق	32	64.0%
محايد	09	18.0%
غير موافق	09	18.0%
الإجمالي	50	100%

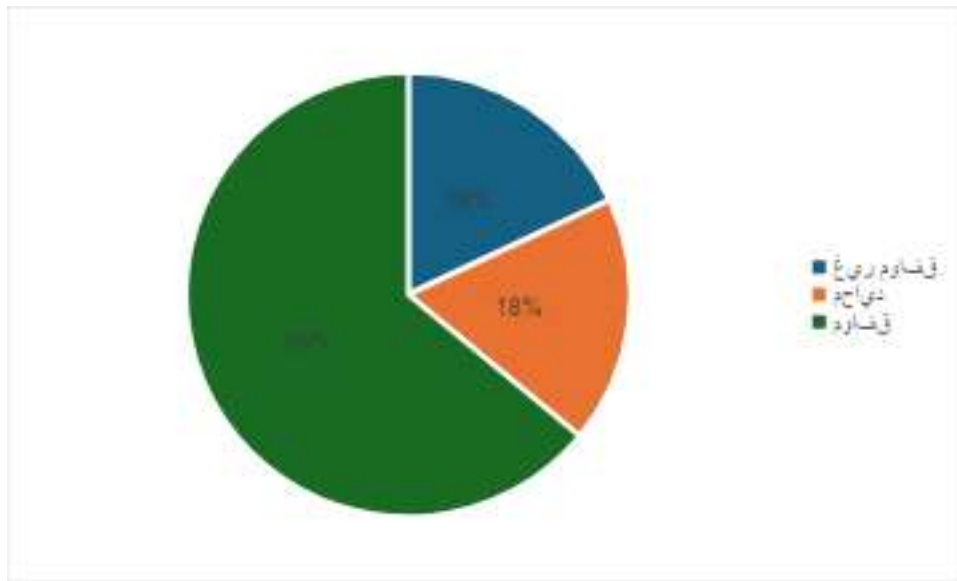
من خلال الجدول أعلاه رقم (05) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (32) فرداً بنسبة مئوية بلغت 64.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (09) أفراد بنسبة 18.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (09) أفراد بنسبة تقدر بـ 18.0%.

تحليل وتفسير :

تشير هذه النتيجة إلى أن أغلبية الطلبة يمتلكون معرفة بالمفاهيم الأساسية المرتبطة بالأمن السيبراني، وهو ما يعكس مستوى مقبولاً من الثقافة الرقمية لديهم، ويمكن تفسير ذلك بطبيعة التخصصات التي ينتمي إليها أفراد العينة، والمتمثلة في الذكاء الاصطناعي وهندسة البرمجيات ونظم المعلومات، حيث تتضمن هذه التخصصات مقررات أكاديمية تعتمد على التعامل مع الأنظمة الرقمية والشبكات وقواعد البيانات، الأمر الذي يساهم في تعزيز معارف الطلبة المتعلقة بالأمن السيبراني.

كما أن الانتشار الواسع للتكنولوجيا الرقمية ووسائل التواصل الاجتماعي والتطبيقات الإلكترونية جعل موضوع الأمن السيبراني جزءاً من الحياة اليومية للطلبة، مما أسهم في رفع مستوى الوعي لديهم بالمفاهيم الأساسية المرتبطة بحماية البيانات والخصوصية الرقمية، وفي المقابل، فإن نسبة المحايدين وغير الموافقين تدل على وجود تفاوت في مستوى المعرفة بين الطلبة، الأمر الذي يمكن أن يرجع إلى اختلاف الخبرات الشخصية ومستوى الاهتمام الفردي بهذا المجال.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (05): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (01)

البند رقم (02):

نص البند رقم (02) على: " أدرك المخاطر التقنية المرتبطة بالتعامل مع الشبكات المفتوحة ومنصات تبادل البيانات."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (06) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (02)

البديل	التكرارات	النسبة المئوية
موافق	37	74.0%
محايد	08	16.0%
غير موافق	05	10.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (06) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (37) فرداً بنسبة مئوية بلغت 74.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (08) أفراد بنسبة 16.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (05) أفراد بنسبة مئوية قدرت بـ 10.0%.

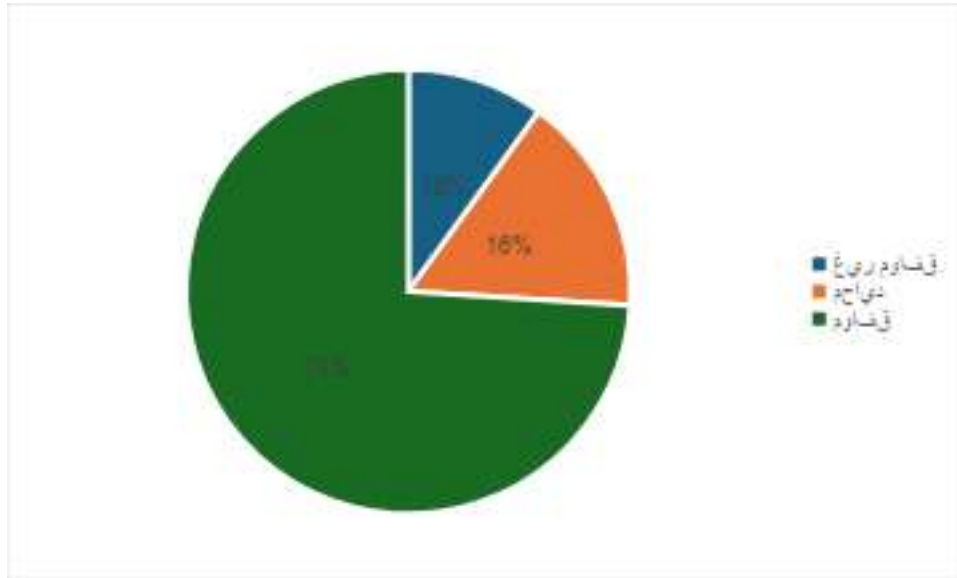
تحليل وتفسير :

أظهرت النتائج أن نسبة الموافقة بلغت 74%، وهي نسبة مرتفعة تعكس إدراكاً جيداً لدى الطلبة للمخاطر التقنية المرتبطة باستخدام الشبكات المفتوحة ومنصات تبادل البيانات، وتدلل هذه النتيجة على أن أغلبية أفراد العينة أصبحوا أكثر وعياً بالتهديدات الإلكترونية التي يمكن أن تنجم عن استخدام الشبكات غير الآمنة، مثل سرقة البيانات الشخصية أو التعرض للاختراقات الإلكترونية.

ويمكن تفسير هذه النتيجة بارتفاع حجم التغطية الإعلامية للقضايا المتعلقة بالأمن السيبراني، حيث أصبحت أخبار الاختراقات والهجمات الإلكترونية جزءاً من المحتوى المتداول عبر وسائل الإعلام التقليدية والرقمية،

كما أن العديد من الطلبة سبق لهم التعامل مع تطبيقات ومنصات رقمية تتطلب إجراءات أمنية مختلفة، مما أكسبهم خبرة عملية ساهمت في رفع مستوى إدراكهم للمخاطر التقنية.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (60) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (02)

البند رقم (03):

نص البند رقم (03) على: "أتابع المنصات الأكاديمية والمواقع التقنية المتخصصة للاطلاع على المستجدات المتعلقة بالأمن السيبراني"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (07) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (03)

البديل	التكرارات	النسبة المئوية
موافق	26	52.0%
محايد	15	30.0%
غير موافق	09	18.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (07) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (26) فرداً بنسبة مئوية بلغت 52.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (15) فرداً بنسبة 30.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (09) أفراد بنسبة تقدر بـ 18.0%.

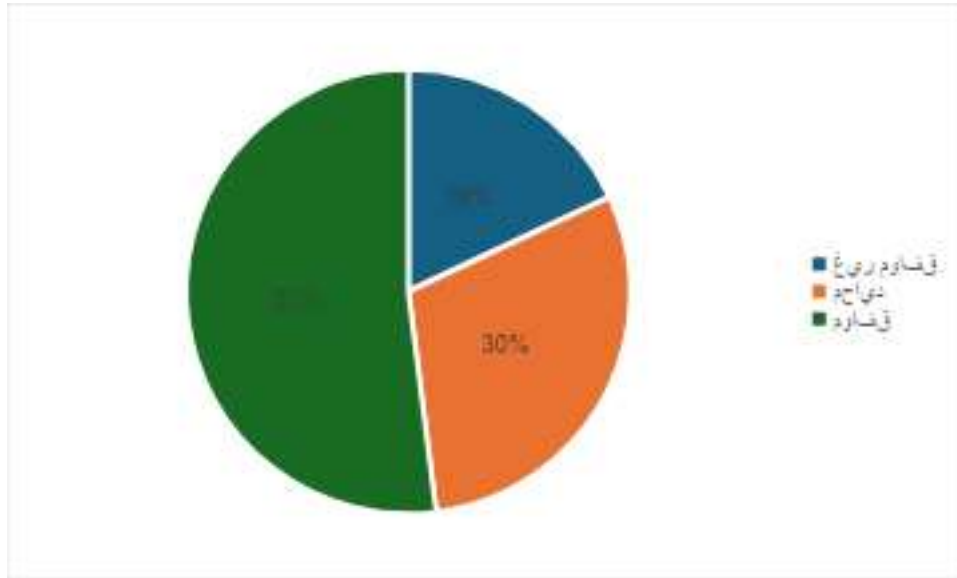
تحليل وتفسير:

تعكس هذه النتيجة وجود مستوى متوسط إلى مرتفع من اهتمام الطلبة بمتابعة المستجدات المتعلقة بالأمن السيبراني عبر المنصات الأكاديمية والمواقع التقنية المتخصصة، حيث إن أكثر من نصف أفراد العينة أكدوا متابعتهم لهذه المصادر، ويُفسر ذلك بطبيعة التخصصات التقنية التي ينتمي إليها الطلبة، والتي تفرض عليهم مواكبة التطورات المتسارعة في مجالات البرمجيات والذكاء الاصطناعي وأمن المعلومات، خاصة وأن التهديدات السيبرانية تتطور باستمرار وتستدعي الاطلاع الدائم على أساليب الحماية الحديثة.

كما يمكن تفسير هذه النتيجة بسهولة الوصول إلى المحتوى الرقمي المتخصص من خلال الإنترنت، ووجود العديد من المنصات التقنية العالمية التي توفر محتويات تعليمية و تدريبية مجانية حول الأمن السيبراني، وأيضاً يشير

ارتفاع نسبة المحايدين نسبياً إلى أن عدداً من الطلبة قد يعتمدون على المعلومات المقدمة داخل الجامعة فقط دون متابعة مستمرة للمصادر المتخصصة، أو قد يواجهون صعوبات تتعلق باللغة أو الوقت أو نقص الدافعية نحو البحث الذاتي.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (07): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (03)

البند رقم (05):

نص البند رقم (05) على: " أعرف أهمية تطبيق إجراءات الأمن السيبراني أثناء استخدام الأنظمة الإلكترونية."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (08) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (05)

البديل	التكرارات	النسبة المئوية
موافق	34	68.0%
محايد	13	26.0%
غير موافق	03	6.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (08) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (34) فرداً بنسبة مئوية بلغت 68.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (13) فرداً بنسبة 26.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (03) أفراد بنسبة مئوية قدرت بـ 6.0%.

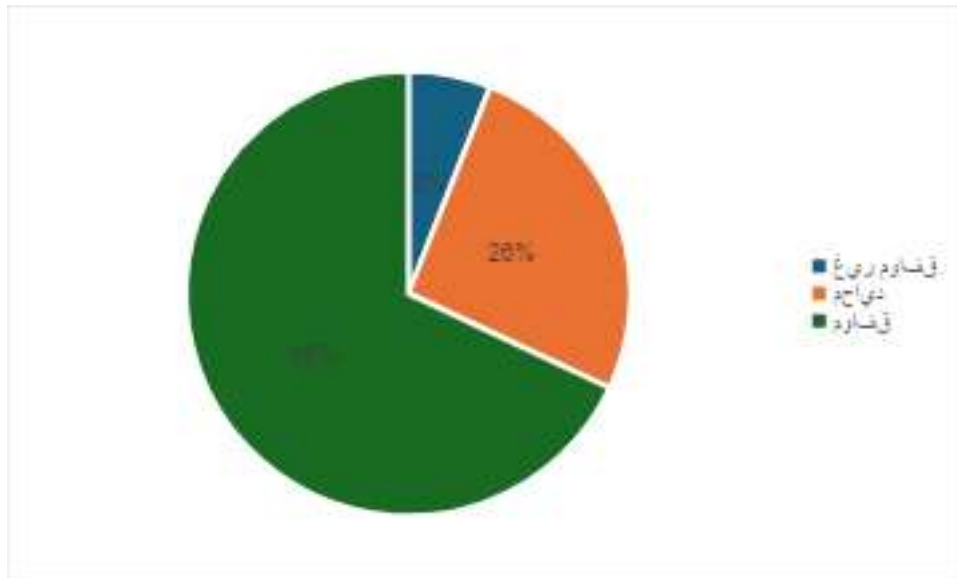
تحليل وتفسير :

تشير هذه النتيجة إلى وجود وعي مرتفع لدى أفراد العينة بأهمية تطبيق إجراءات الأمن السيبراني أثناء استخدام الأنظمة الإلكترونية المختلفة، وهو ما يعكس إدراكهم للدور الذي تؤديه هذه الإجراءات في حماية المعلومات والأنظمة من الاختراقات والتهديدات الرقمية.

ويمكن تفسير هذه النتيجة بأن الطلبة أصبحوا يتعاملون بشكل يومي مع العديد من الخدمات الإلكترونية والمنصات الرقمية التي تتطلب الالتزام بإجراءات أمنية مختلفة مثل كلمات المرور القوية والمصادقة الثنائية وتحديث البرامج، مما جعلهم أكثر إدراكاً لأهمية الأمن السيبراني في حياتهم الأكاديمية والشخصية.

كما أن التغطية الإعلامية المتزايدة لحوادث الاختراق والتسريب الإلكتروني أسهمت في رفع مستوى الوعي بأهمية تطبيق الإجراءات الوقائية، أما نسبة الحياد فتشير إلى أن بعض الطلبة يدركون أهمية الأمن السيبراني من الناحية النظرية، لكنهم قد لا يمتلكون تصوراً واضحاً أو شاملاً لجميع الإجراءات الأمنية المطلوبة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (08): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (05)

البند رقم (06):

نص البند رقم (06) على: " أمتلك مهارة التعامل مع إعدادات الأمان المتقدمة لضمان سلامة البيانات الرقمية.."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (09) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (06)

البديل	التكرارات	النسبة المئوية
موافق	24	48.0%
محايد	10	20.0%
غير موافق	16	32.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (09) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (24) فرداً بنسبة مئوية بلغت 48.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (10) أفراد بنسبة 20.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (16) فرداً بنسبة تقدر بـ 32.0%.

تحليل وتفسير:

تكشف هذه النتيجة عن وجود تفاوت واضح بين المعرفة النظرية والمهارات التطبيقية المتعلقة بالأمن السيبراني، فعلى الرغم من أن نسبة الموافقة هي الأعلى، إلا أن نسبة غير الموافقين مرتفعة نسبياً، مما يدل على أن جزءاً مهماً من الطلبة لا يمتلكون الكفاءة الكافية للتعامل مع الإعدادات الأمنية المتقدمة.

ويمكن تفسير ذلك بأن التعامل مع إعدادات الأمان المتقدمة يتطلب خبرة تقنية وتدريباً عملياً يفوق المعرفة العامة بمفاهيم الأمن السيبراني، وهو ما قد لا يتوفر لجميع الطلبة بدرجة متساوية، كما أن بعض إعدادات الحماية المتقدمة تتطلب فهماً للشبكات وأنظمة التشغيل وإدارة الصلاحيات والتشفير، وهي مهارات قد تكون أكثر انتشاراً لدى طلبة بعض التخصصات مقارنة بغيرهم.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (09): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (06)

البند رقم (07):

نص البند رقم (07) على: " أدرك المخاطر الأمنية المرتبطة بنماذج الذكاء الاصطناعي، مثل احتمالية تزييف البيانات أو اختراق الخوارزميات (Model Poisoning) لتضليل النتائج.

"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (10) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (07)

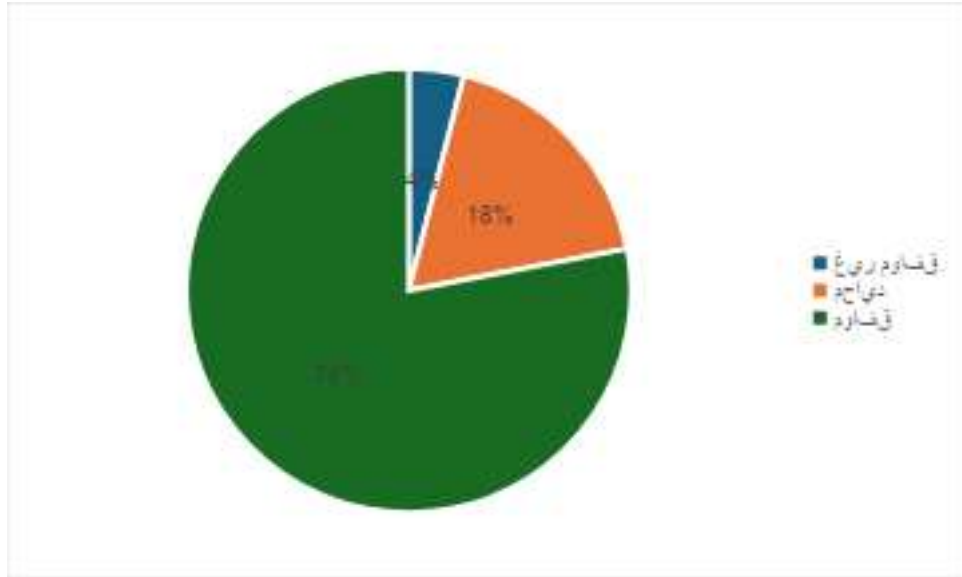
البديل	التكرارات	النسبة المئوية
موافق	39	78.0%
محايد	09	18.0%
غير موافق	02	4.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (10) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (39) فرداً بنسبة مئوية بلغت 78.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (09) أفراد بنسبة 18.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (02) فرد بنسبة مئوية قدرت بـ 4.0%.

تحليل وتفسير:

بينت هذه النتيجة مستوى مرتفعاً جداً من الوعي بالمخاطر الأمنية المرتبطة بتقنيات الذكاء الاصطناعي، وهو أمر متوقع بالنظر إلى طبيعة تخصصات أفراد العينة التي تتضمن الذكاء الاصطناعي وهندسة البرمجيات ونظم المعلومات.

كما يمكن تفسير هذه النتيجة بالانتشار الواسع للنقاشات العلمية والإعلامية حول المخاطر المرتبطة بالذكاء الاصطناعي، مثل التزييف العميق (Deepfake) وهجمات تسميم البيانات (Data Poisoning) والتلاعب بالنماذج الذكية، وقد ساهم ذلك في رفع مستوى إدراك الطلبة لهذه المخاطر، خاصة مع تزايد الاعتماد على تقنيات الذكاء الاصطناعي في مختلف المجالات.



وتدل هذه النتيجة على أن الطلبة لا ينظرون إلى الذكاء الاصطناعي باعتباره تقنية مفيدة فقط، بل يدركون أيضاً التحديات والتهديدات الأمنية المصاحبة له، وهو مؤشر إيجابي على نضج الوعي التقني لديهم. وهذا ما هو موضح في الشكل التالي:

الشكل رقم (10): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (07)

المحور الثاني: مصادر الوعي بالأمن السيبراني

البند رقم (08):

نص البند رقم (08) على: ". يساهم التكوين الجامعي في تعزيز وعيي بأسس الامن السيبراني "، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (11) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (08)

البديل	التكرارات	النسبة المئوية
موافق	27	54.0%
محايد	06	12.0%
غير موافق	17	34.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (11) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (27) فرداً بنسبة مئوية بلغت 54.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (06) أفراد بنسبة 12.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (17) فرداً بنسبة تقدر بـ 34.0%.

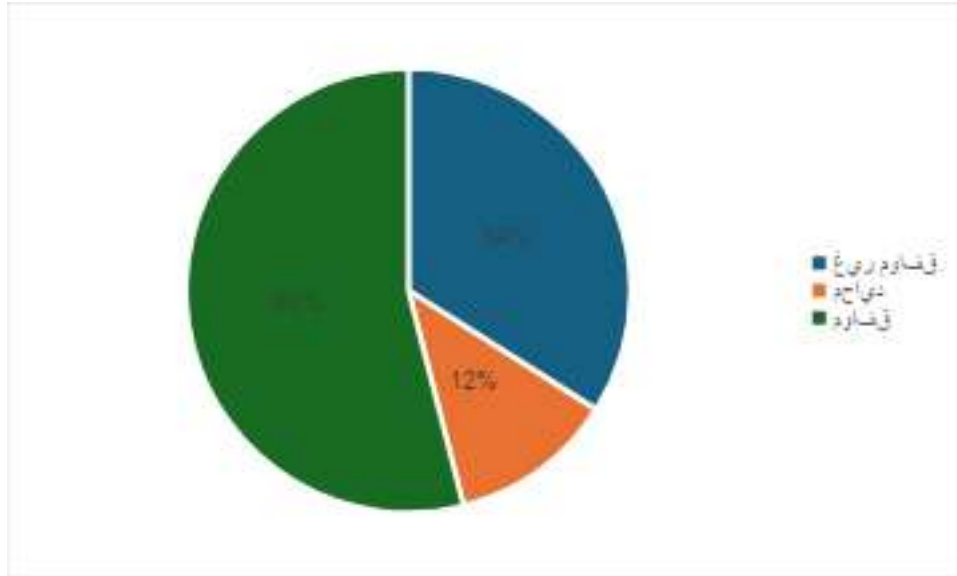
تحليل وتفسير :

تشير هذه النتيجة إلى أن أكثر من نصف أفراد العينة يرون أن التكوين الجامعي يساهم في تعزيز وعيهم بأساسيات الأمن السيبراني، وهو ما يعكس الدور الإيجابي الذي تؤديه الجامعة في تزويد الطلبة بالمفاهيم والمعارف المرتبطة بحماية المعلومات والأنظمة الرقمية، ويعود ذلك إلى احتواء البرامج التعليمية على بعض المقررات والأنشطة التي تتناول الجوانب التقنية المتعلقة بالشبكات وقواعد البيانات وأمن المعلومات.

غير أن ارتفاع نسبة غير الموافقين إلى 34.0% يكشف عن وجود شعور لدى شريحة معتبرة من الطلبة بأن التكوين الجامعي لا يلبي بشكل كاف احتياجاتهم المعرفية في مجال الأمن السيبراني، ويمكن تفسير ذلك بالتطور

السريع لهذا المجال مقارنة بسرعة تحديث المناهج الدراسية، إضافة إلى محدودية التطبيقات العملية المتخصصة في بعض البرامج الأكاديمية.

وتشير هذه النتيجة إلى أن الجامعة تؤدي دوراً مهماً في بناء الوعي السيبراني، إلا أن هذا الدور ما يزال بحاجة إلى مزيد من التطوير من خلال تحديث البرامج التعليمية وإدراج محتويات أكثر تخصصاً في الأمن السيبراني وهذا ما هو موضح في الشكل التالي:



الشكل رقم (11): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (08)

البند رقم (09):

نص البند رقم (09) على: " تساهم المواقع التقنية والمنصات العلمية المتخصصة في زيادة إدراكي للمخاطر السيبرانية المعاصرة"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (12) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (09)

البديل	التكرارات	النسبة المئوية
موافق	31	62.0%
محايد	09	18.0%
غير موافق	10	20.0%
الإجمالي	50	100%

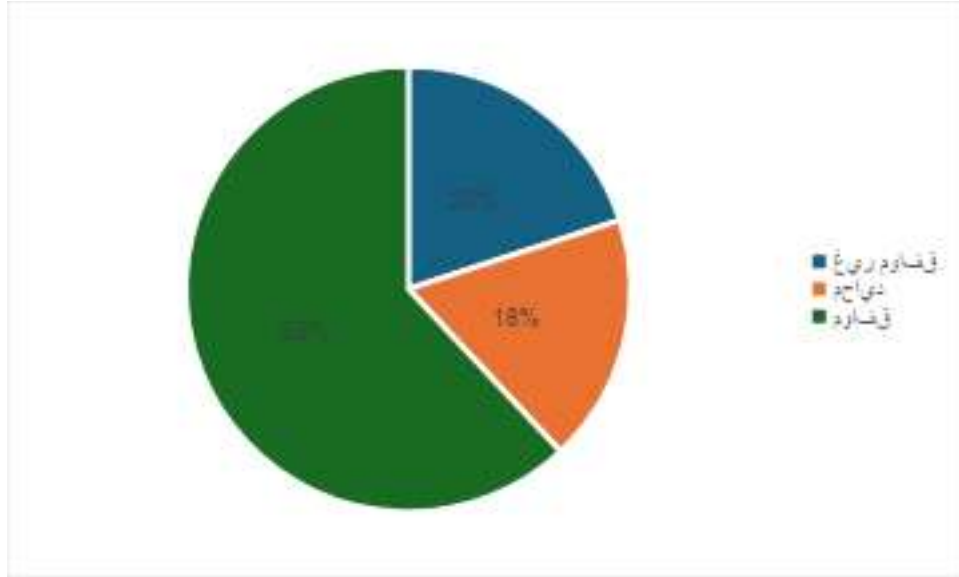
من خلال الجدول أعلاه رقم (12) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (31) فرداً بنسبة مئوية بلغت 62.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (09) أفراد بنسبة 18.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (10) أفراد بنسبة مئوية قدرت بـ 20.0%.

تحليل وتفسير :

تعكس هذه النتيجة الدور البارز الذي تؤديه المواقع التقنية والمنصات العلمية في تنمية وعي الطلبة بالمخاطر السيبرانية الحديثة، حيث يرى أغلب أفراد العينة أن هذه المصادر تساعدهم على فهم التهديدات الإلكترونية المستجدة وأساليب مواجهتها.

ويرجع ذلك إلى أن هذه المنصات تتميز بسرعة نشر المعلومات والتحديثات المتعلقة بالثغرات الأمنية والهجمات الإلكترونية، الأمر الذي يجعلها مصدراً مهماً للمعلومات الحديثة مقارنة بالمصادر التقليدية، كما أن الطلبة في التخصصات التقنية يميلون بطبيعتهم إلى البحث عن المعلومات عبر الإنترنت والاستفادة من المحتويات العلمية المتخصصة.

أما نسبة غير الموافقين فقد تعود إلى محدودية متابعة بعض الطلبة لهذه المنصات أو اعتمادهم بشكل أكبر على المصادر الجامعية التقليدية، ومع ذلك فإن النتيجة تؤكد الأهمية المتزايدة للمصادر الرقمية في بناء الوعي السبيري لدى الطلبة الجامعيين، وهذا ما هو موضح في الشكل التالي:



الشكل رقم (12): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (09)

البند رقم (10):

نص البند رقم (10) على: " أستفيد من المنصات التقنية والمجتمعات البرمجية في متابعة قضايا الأمن السيبراني."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (13) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (10)

البديل	التكرارات	النسبة المئوية
موافق	30	60.0%
محايد	16	32.0%
غير موافق	04	8.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (13) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (30) فرداً بنسبة مئوية بلغت 60.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (16) فرداً بنسبة 32.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (04) أفراد بنسبة تقدر بـ 8.0%.

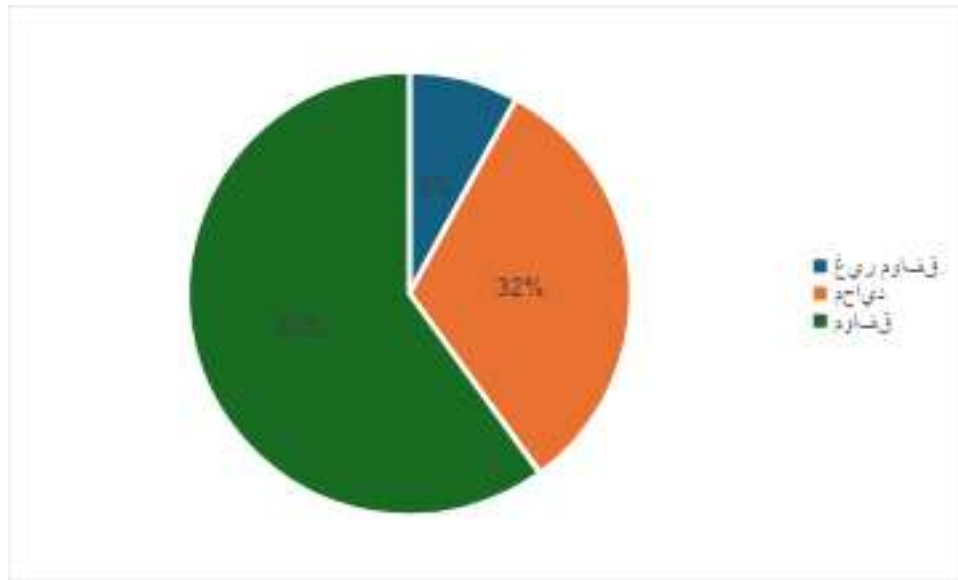
تحليل وتفسير:

تدل هذه النتيجة على أن غالبية الطلبة يستفيدون من المجتمعات التقنية والبرمجية في متابعة المستجدات المتعلقة بالأمن السيبراني، وهو ما يعكس أهمية التعلم الذاتي والتفاعل مع المجتمعات الرقمية المتخصصة في تطوير المعارف التقنية.

ويمكن تفسير هذه النتيجة بانتشار المنصات التعليمية والمجتمعات البرمجية التي تتيح تبادل الخبرات والمعارف بين المبرمجين والمتخصصين في المجال التقني، حيث توفر هذه البيئات فرصاً للتعلم المستمر ومواكبة التطورات الحديثة.

أما ارتفاع نسبة المحايدين نسبياً فيشير إلى أن بعض الطلبة لا يشاركون بشكل منتظم في هذه المجتمعات أو لا يعتمدون عليها كمصدر أساسي للمعرفة، وهو ما يستدعي تشجيع الطلبة على الانخراط بشكل أكبر في البيئات الرقمية المتخصصة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (13): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (10)

البند رقم (11):

نص البند رقم (11) على: " تغطي المحاضرات والدروس الجامعية الجوانب التقنية والبرمجية للأمن السيبراني بشكل كافٍ"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (14) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (11)

البديل	التكرارات	النسبة المئوية
موافق	13	26.0%
محايد	10	20.0%
غير موافق	27	54.0%
الإجمالي	50	100%

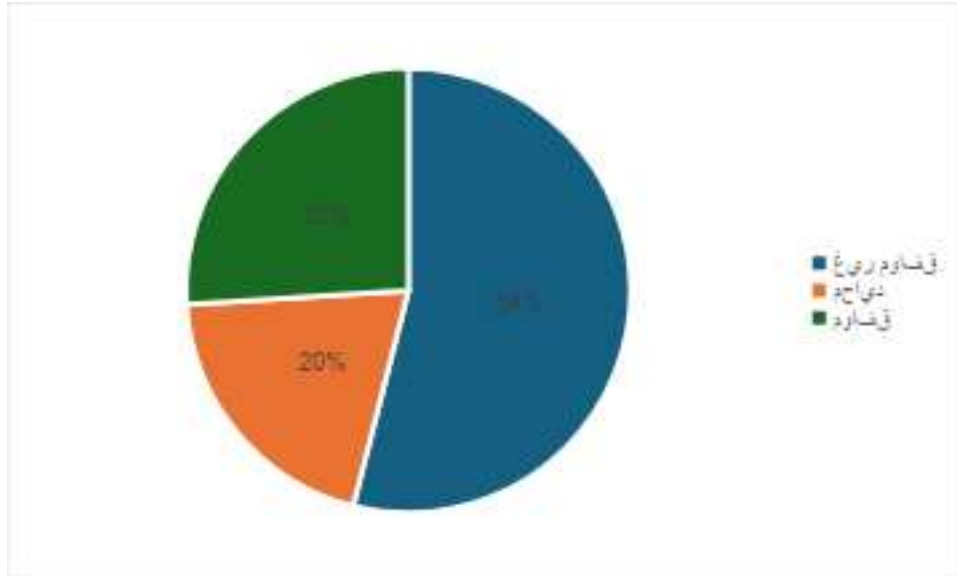
من خلال الجدول أعلاه رقم (14) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (13) فرداً بنسبة مئوية بلغت 26.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (10) أفراد بنسبة 20.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (27) فرداً بنسبة تقدر بـ 54.0%.

تحليل وتفسير :

تعكس هذه النتيجة وجود اتجاه سلبي واضح لدى الطلبة تجاه مدى كفاية المحتوى الجامعي المرتبط بالجوانب التقنية والبرمجية للأمن السيبراني، حيث يرى أكثر من نصف أفراد العينة أن المحاضرات والدروس المقدمة لا تغطي هذا المجال بالشكل المطلوب.

ويمكن تفسير هذه النتيجة بالطبيعة المتجددة للأمن السيبراني، إذ يشهد هذا المجال تطورات متسارعة تتطلب تحديثاً مستمراً للمقررات الدراسية. كما قد تعود هذه النتيجة إلى تركيز بعض البرامج الأكاديمية على الجوانب النظرية أكثر من الجوانب التطبيقية، مما يجعل الطلبة يشعرون بوجود فجوة بين ما يتعلمونه داخل الجامعة وما يتطلبه الواقع المهني.

وتشير هذه النتيجة إلى ضرورة مراجعة البرامج التعليمية وإثرائها بمحتويات أكثر تخصصاً وتطبيقية في مجال الأمن السيبراني، بما يتناسب مع متطلبات البيئة الرقمية الحديثة وهذا ما هو موضح في الشكل التالي:



الشكل رقم (14): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (11)

البند رقم (12):

نص البند رقم (12) على: "تساهم المصادر الأكاديمية والمراجع العلمية في تطوير معرفتي بالأمن السيبراني.."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (15) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (12)

البديل	التكرارات	النسبة المئوية
موافق	27	54.0%
محايد	17	34.0%
غير موافق	06	12.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (15) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (27) فرداً بنسبة مئوية بلغت 54.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (17) فرداً بنسبة 34.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (06) أفراد بنسبة مئوية قدرت بـ 12.0%.

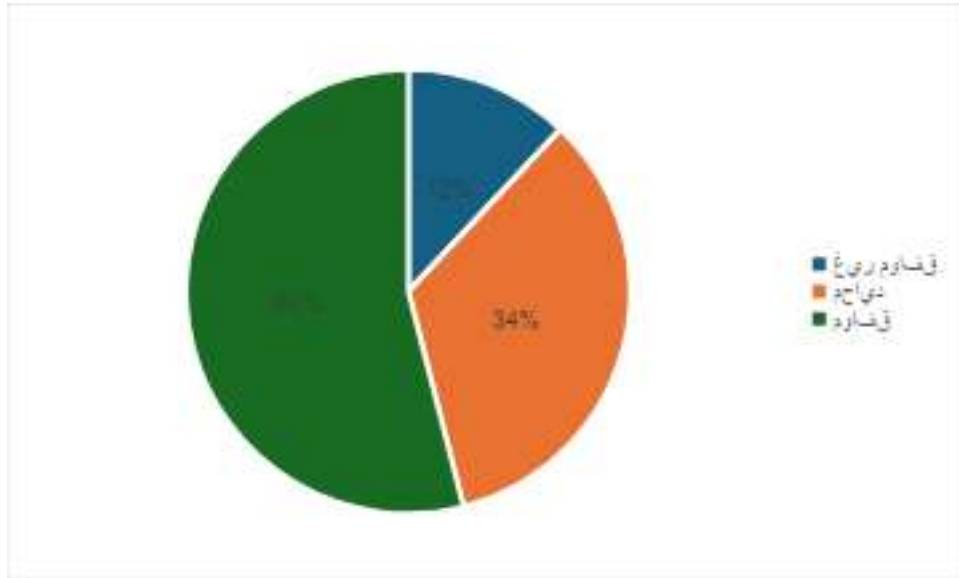
تحليل وتفسير

تشير هذه النتيجة إلى أن أغلبية الطلبة يرون أن المصادر الأكاديمية والمراجع العلمية تساهم في تطوير معارفهم المتعلقة بالأمن السيبراني، وهو ما يؤكد أهمية الكتاب الجامعي والمقالات العلمية والبحوث الأكاديمية في بناء المعرفة المتخصصة.

ويعود ذلك إلى أن هذه المصادر تتميز بالمصداقية والدقة العلمية، كما توفر للطلبة أساساً نظرياً متيناً يساعدهم على فهم المفاهيم والمبادئ المرتبطة بالأمن السيبراني بصورة منهجية، أما ارتفاع نسبة المحايدين نسبياً فقد يعكس ضعف اعتماد بعض الطلبة على القراءة العلمية المنتظمة أو تفضيلهم للمصادر الرقمية السريعة والمبسطة مقارنة بالمراجع الأكاديمية التقليدية.

وتؤكد هذه النتيجة أهمية تعزيز ثقافة البحث العلمي وتشجيع الطلبة على الاستفادة من قواعد البيانات العلمية والمصادر الأكاديمية المتخصصة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (15): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (12)

البند رقم (13):

نص البند رقم (13) على: " أكتسب مهارات حماية الأنظمة والبيانات من خلال التطبيق العملي في المخابر الجامعية والتدريبات التقنية المتخصصة."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (16) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (13)

البديل	التكرارات	النسبة المئوية
موافق	17	34.0%
محايد	13	26.0%
غير موافق	20	40.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (16) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (17) فرداً بنسبة مئوية بلغت 34.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (13) فرداً بنسبة 26.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (20) فرداً بنسبة تقدر بـ 40.0%.

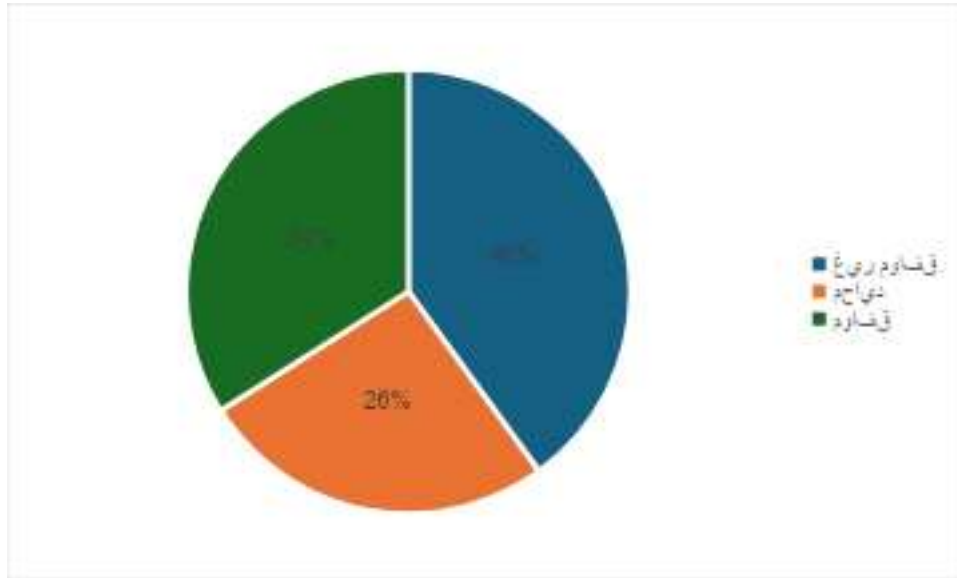
تحليل وتفسير:

تعكس هذه النتيجة وجود قصور نسبي في الجانب التطبيقي المرتبط بالأمن السيبراني داخل البيئة الجامعية، حيث يرى عدد معتبر من الطلبة أن المخابر الجامعية والتدريبات التقنية الحالية لا تمكنهم بالشكل الكافي من اكتساب المهارات العملية اللازمة لحماية الأنظمة والبيانات.

ويمكن تفسير هذه النتيجة بمحدودية التجهيزات التقنية المتخصصة أو قلة الورشات التطبيقية الموجهة للأمن السيبراني، إضافة إلى التركيز النسبي على الجوانب النظرية في بعض البرامج التعليمية، كما أن اكتساب المهارات العملية في هذا المجال يتطلب بيئات تدريبية تحاكي الهجمات والاختراقات الحقيقية، وهو ما قد لا يكون متوفراً بشكل دائم.

وتبرز هذه النتيجة الحاجة الملحة إلى تطوير المخابر التقنية وتكثيف التدريبات التطبيقية المتخصصة، بما يسمح للطلبة بتحويل معارفهم النظرية إلى مهارات عملية قابلة للتطبيق في الواقع المهني.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (16): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (13)

المحور الثالث: الممارسات والسلوكيات الرقمية للطلبة

البند رقم (14):

نص البند رقم (14) على: " استخدام تقنيات المصادقة الثنائية وإدارة كلمات المرور المعقدة لتأمين الوصول الى حساباتي"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (17) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (14)

البديل	التكرارات	النسبة المئوية
موافق	35	70.0%
محايد	07	14.0%
غير موافق	08	16.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (17) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (35) فرداً بنسبة مئوية بلغت 70.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (07) أفراد بنسبة 14.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (08) أفراد بنسبة مئوية قدرت بـ 16.0%.

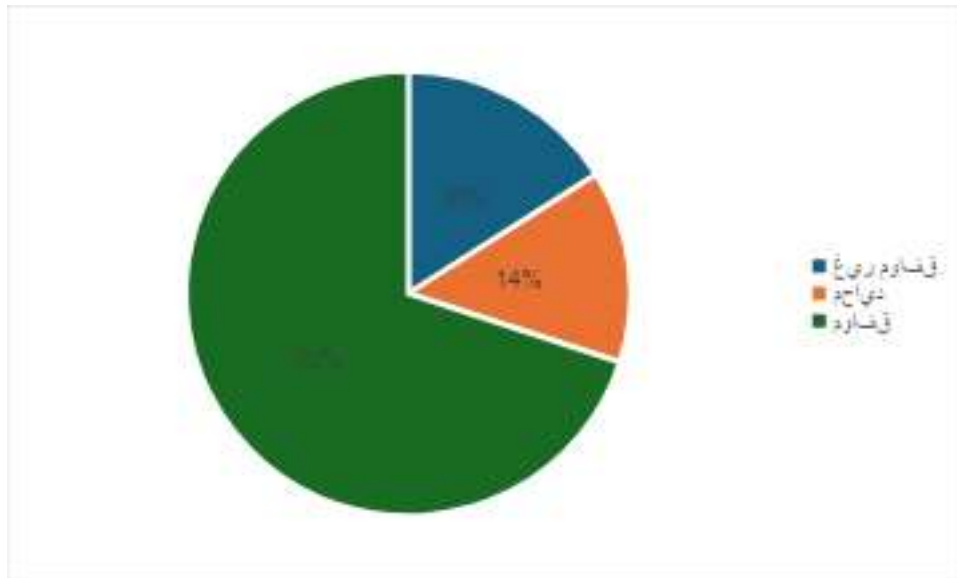
تحليل وتفسير :

تشير هذه النتيجة إلى أن أغلبية الطلبة يطبقون أحد أهم الممارسات الأساسية في الأمن السيبراني، والمتمثلة في استخدام المصادقة الثنائية وكلمات المرور القوية لحماية حساباتهم الرقمية، ويعكس ذلك ارتفاع مستوى الوعي بالمخاطر المرتبطة بسرقة الحسابات الشخصية والاختراقات الإلكترونية التي أصبحت من أكثر التهديدات شيوعاً في البيئة الرقمية المعاصرة.

كما يمكن تفسير هذه النتيجة بالانتشار الواسع لخدمات المصادقة الثنائية التي توفرها مختلف المنصات الإلكترونية، بالإضافة إلى الحملات التوعوية التي تشجع المستخدمين على تعزيز حماية حساباتهم، ويسهم التكوين

التقني للطلبة أيضاً في إدراكهم لأهمية هذه الإجراءات الوقائية في الحد من مخاطر الوصول غير المصرح به إلى البيانات الشخصية.

أما نسبة غير الموافقين فتشير إلى أن بعض الطلبة ما زالوا يعتمدون على وسائل حماية تقليدية، وهو ما يستدعي تكثيف الجهود التوعوية لتعزيز تبني الممارسات الأمنية الحديثة. وهذا ما هو موضح في الشكل التالي:



الشكل رقم (17): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (14)

البند رقم (15):

نص البند رقم (15) على: " أجنب مشاركة بيانات الاعتماد (Credentials) أو الأكواد البرمجية الخاصة عبر المنصات غير المشفرة."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (18) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (15)

البديل	التكرارات	النسبة المئوية
موافق	28	56.0%
محايد	17	34.0%
غير موافق	05	10.0%
الإجمالي	50	100%

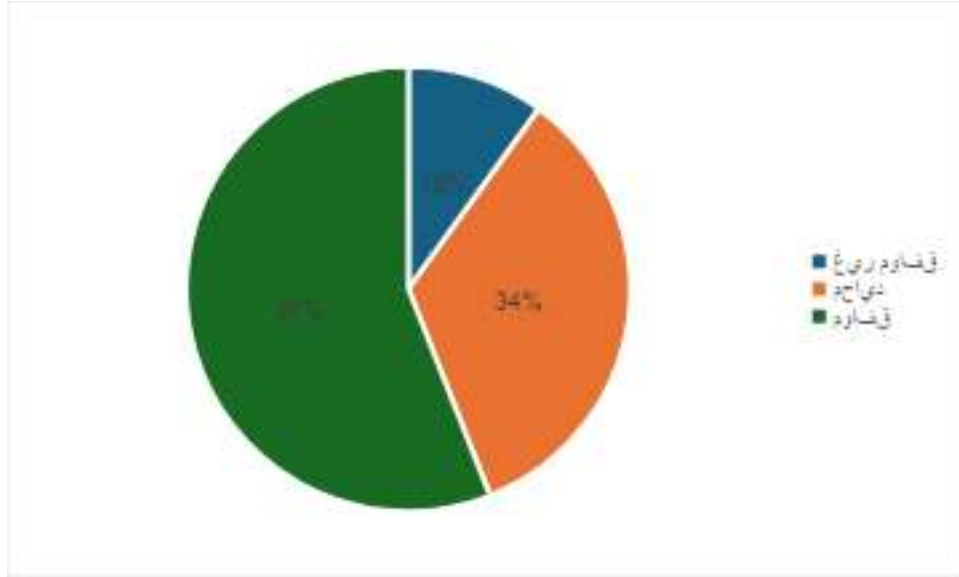
من خلال الجدول أعلاه رقم (18) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (28) فرداً بنسبة مئوية بلغت 56.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (17) فرداً بنسبة 34.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (05) أفراد بنسبة تقدر بـ 10.0%.

تحليل وتفسير :

تعكس هذه النتيجة وجود وعي جيد لدى الطلبة بأهمية المحافظة على سرية بيانات الاعتماد والمعلومات الحساسة وعدم مشاركتها عبر القنوات غير الآمنة، ويُعد هذا السلوك من الممارسات الأساسية التي تقلل من احتمالية التعرض للاختراق أو تسريب المعلومات الشخصية والمهنية.

ويمكن تفسير هذه النتيجة بإدراك الطلبة لطبيعة المخاطر المرتبطة بعمليات نقل البيانات عبر منصات غير محمية، خاصة مع تزايد الحوادث المرتبطة بسرقة الحسابات واستغلال المعلومات المسربة، كما أن تخصصات العينة تجعلهم أكثر احتكاً بالمفاهيم المتعلقة بسرية المعلومات وحماية البيانات.

أما نسبة المحايدين المرتفعة نسبياً فقد تدل على أن بعض الطلبة لا يلتزمون دائماً بهذه الممارسة أو لا يدركون جميع المخاطر المرتبطة بمشاركة المعلومات الحساسة عبر القنوات غير الآمنة. وهذا ما هو موضح في الشكل التالي:



الشكل رقم (18): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (15)

البند رقم (16):

نص البند رقم (16) على: " أقوم بفحص عناوين الروابط (URLs) بدقة للتأكد من خلوها من محاولات التصيد الاحتيالي قبل التفاعل معها."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (19) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (16)

البديل	التكرارات	النسبة المئوية
موافق	26	52.0%
محايد	14	28.0%
غير موافق	10	20.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (19) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (26) فرداً بنسبة مئوية بلغت 52.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (14) فرداً بنسبة 28.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (10) أفراد بنسبة مئوية قدرت بـ 20.0%.

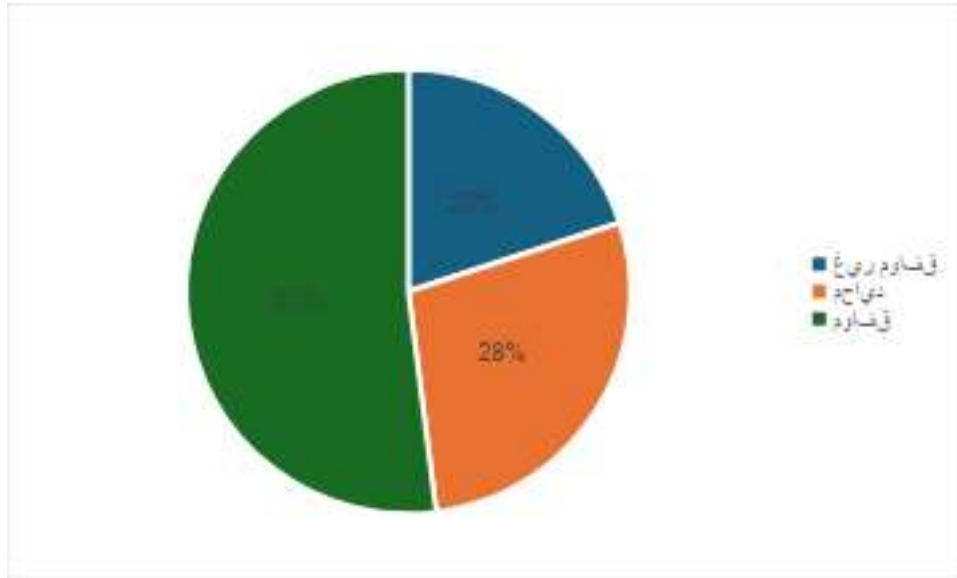
تحليل وتفسير :

تشير هذه النتيجة إلى أن أكثر من نصف أفراد العينة يمتلكون سلوكاً وقائياً يتمثل في التحقق من الروابط الإلكترونية قبل التعامل معها، وهو ما يعكس وعياً بمخاطر التصيد الاحتيالي الذي يعد من أكثر أساليب الهجمات الإلكترونية انتشاراً.

ويمكن تفسير هذه النتيجة بازدياد الحملات التوعوية التي تحذر من الروابط المزيفة ورسائل الاحتيال الإلكتروني، إضافة إلى الخبرات السابقة لبعض الطلبة في التعامل مع محاولات التصيد، كما أن المعرفة التقنية تساعدهم على اكتشاف المؤشرات التي قد تدل على عدم موثوقية الرابط.

إلا أن وجود نسبة معتبرة من المحايدين وغير الموافقين يكشف عن الحاجة إلى مزيد من التدريب العملي على اكتشاف الروابط المشبوهة، خاصة أن نجاح هجمات التصيد يعتمد غالباً على ضعف انتباه المستخدم أو نقص خبرته التقنية.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (19): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (16)

البند رقم (17):

نص البند رقم (17) على: "أستخدم برامج الحماية وتحديث الأنظمة بشكل دوري"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (20) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (17)

البديل	التكرارات	النسبة المئوية
موافق	32	64.0%
محايد	11	22.0%
غير موافق	07	14.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (20) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (32) فرداً بنسبة مئوية بلغت 64.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (11) فرداً بنسبة 22.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (07) أفراد بنسبة تقدر بـ 14.0%.

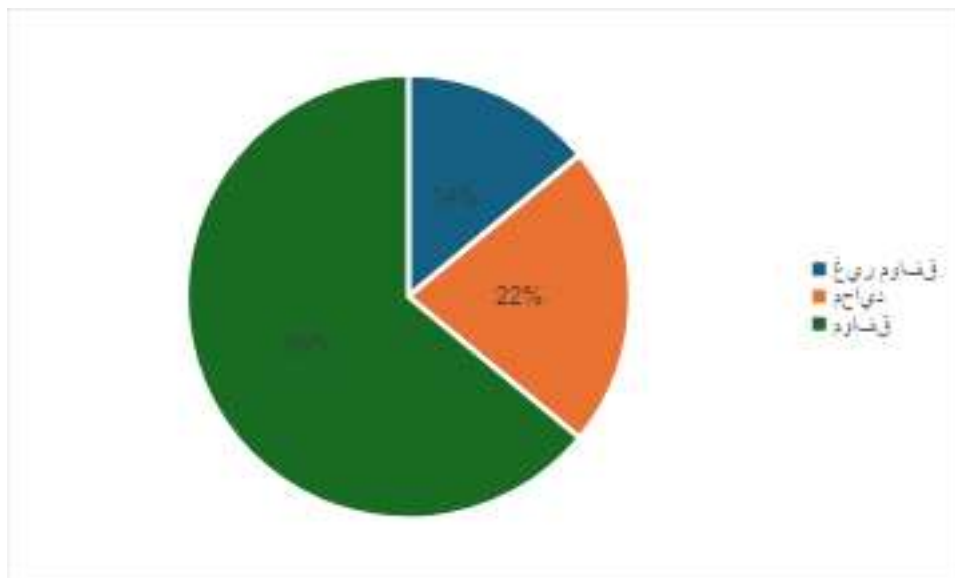
تحليل وتفسير :

تعكس هذه النتيجة تبني أغلبية الطلبة لسلوكيات وقائية مهمة تتمثل في استخدام برامج الحماية والحرص على تحديث الأنظمة بشكل دوري، وهو ما يساهم في تقليل فرص استغلال الثغرات الأمنية من قبل المهاجمين.

ويمكن تفسير هذه النتيجة بانتشار الوعي بأهمية التحديثات الأمنية التي تصدرها الشركات المطورة للبرمجيات، فضلاً عن إدراك الطلبة لأهمية برامج مكافحة الفيروسات وأدوات الحماية الرقمية في مواجهة البرمجيات الخبيثة والهجمات الإلكترونية المختلفة.

كما تشير النتيجة إلى أن الطلبة أصبحوا أكثر اقتناعاً بأن الأمن السيبراني لا يقتصر على المعرفة النظرية، بل يتطلب ممارسات عملية مستمرة للحفاظ على سلامة الأجهزة والبيانات.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (20): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (17)

البند رقم (18):

نص البند رقم (18) على: " ألتزم بتطبيق مبادئ 'الأمن منذ التصميم' (Security by Design) عند بناء النظم البرمجية، مع التركيز على تأمين واجهات البرمجة (APIs) ومنع تسريب البيا"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (21) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (18)

البديل	التكرارات	النسبة المئوية
موافق	24	48.0%
محايد	18	36.0%
غير موافق	08	16.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (21) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (24) فرداً بنسبة مئوية بلغت 48.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (18) فرداً بنسبة 36.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (08) أفراد بنسبة مئوية قدرت بـ 16.0%.

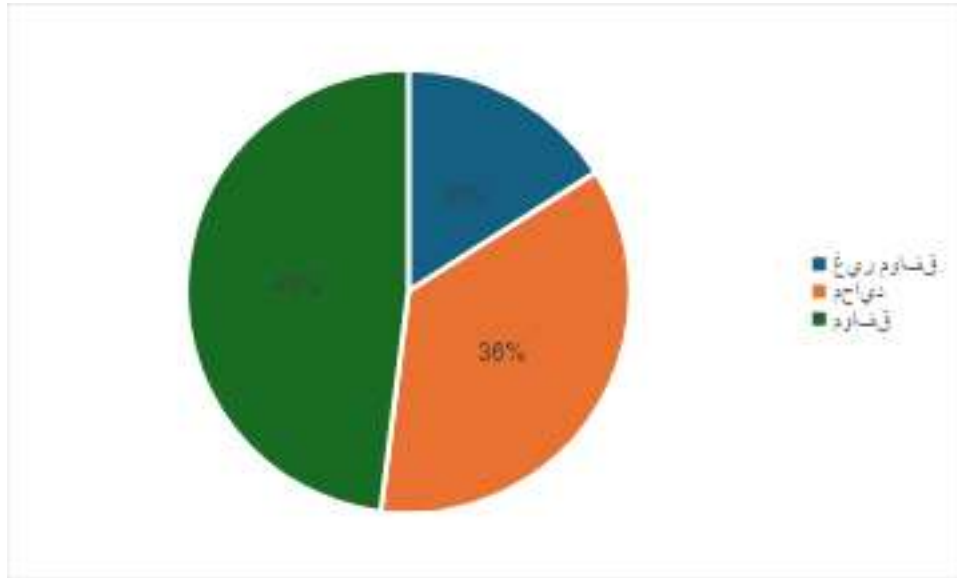
تحليل وتفسير :

تشير هذه النتيجة إلى أن الطلبة يمتلكون مستوى متوسطاً من الالتزام بالممارسات الأمنية المتقدمة المرتبطة بتطوير البرمجيات، فمفهوم "الأمن منذ التصميم" يعد من المفاهيم المتخصصة التي تتطلب فهماً عميقاً لدورة حياة تطوير البرمجيات وآليات الحماية المدججة داخل الأنظمة.

ويمكن تفسير هذه النتيجة بأن هذا المفهوم يرتبط أكثر بالجانب التطبيقي والمهني مقارنة بالمفاهيم العامة للأمن السيبراني، لذلك قد لا يكون جميع الطلبة قد اكتسبوا الخبرة الكافية لتطبيقه فعلياً أثناء تطوير المشاريع البرمجية.

كما أن ارتفاع نسبة المحايدين يدل على وجود شريحة من الطلبة تدرك أهمية هذا المبدأ نظرياً لكنها لم تتح لها فرص كافية لتطبيقه عملياً، وهو ما يعكس الحاجة إلى تعزيز المشاريع التطبيقية والتدريبات البرمجية المتخصصة

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (21): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (18)

البند رقم (19):

نص البند رقم (19) على: " أتحقق من صلاحيات الوصول Permissions التي تتطلبها التطبيقات قبل تثبيتها على جهازي لضمان خصوصية البيانات " ، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (22) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (19)

البديل	التكرارات	النسبة المئوية
موافق	37	74.0%
محايد	11	22.0%
غير موافق	02	4.0%
الإجمالي	50	100%

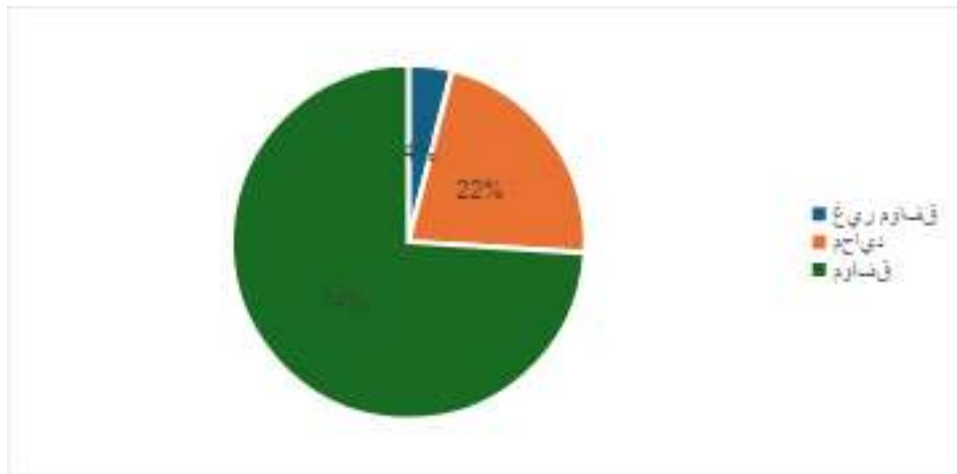
من خلال الجدول أعلاه رقم (22) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (37) فرداً بنسبة مئوية بلغت 74.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (11) فرداً بنسبة 22.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (02) فرد بنسبة تقدر بـ 4.0%.

تحليل وتفسير :

تعكس هذه النتيجة مستوى مرتفعاً من الوعي الرقمي لدى الطلبة فيما يتعلق بحماية الخصوصية الشخصية، حيث يدرك أغلبهم أن بعض التطبيقات قد تطلب صلاحيات غير ضرورية يمكن أن تشكل تهديداً لسرية البيانات.

ويمكن تفسير هذه النتيجة بالانتشار المتزايد للنقاشات المتعلقة بخصوصية المستخدمين واستغلال البيانات الشخصية من قبل بعض التطبيقات والمنصات الرقمية، مما جعل المستخدمين أكثر حرصاً على مراقبة الأذونات الممنوحة للتطبيقات.

كما تشير هذه النتيجة إلى أن الطلبة أصبحوا أكثر وعياً بحقوقهم الرقمية وأكثر قدرة على اتخاذ قرارات أمنية تساهم في حماية معلوماتهم الشخصية، وهذا ما هو موضح في الشكل التالي:



الشكل رقم (22): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (19)

البند رقم (20):

نص البند رقم (20) على: "أُتجذب تبادل بيانات غير مشفرة أو الدخول إلى أنظمة حساسة عند الاتصال بشبكات Wi-Fi العامة"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (23) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (20)

البديل	التكرارات	النسبة المئوية
موافق	36	72.0%
محايد	08	16.0%
غير موافق	06	12.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (23) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (36) فرداً بنسبة مئوية بلغت 72.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (08) أفراد بنسبة 16.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (06) أفراد بنسبة مئوية قدرت بـ 12.0%.

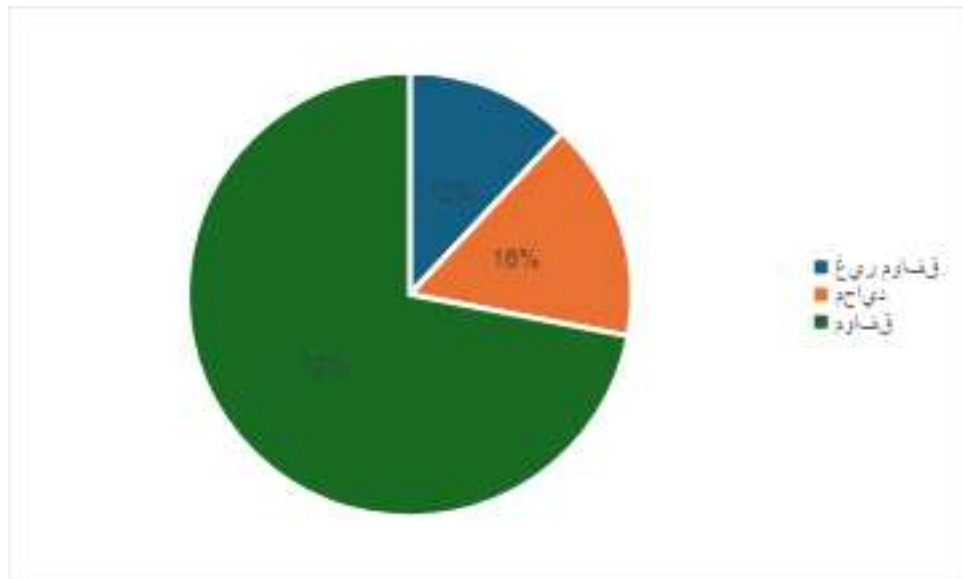
تحليل وتفسير:

تدل هذه النتيجة على أن غالبية الطلبة يدركون المخاطر الأمنية المرتبطة باستخدام الشبكات العامة غير المؤمنة، ويحرصون على تجنب إجراء العمليات الحساسة أو تبادل البيانات المهمة أثناء الاتصال بها.

ويمكن تفسير هذه النتيجة بزيادة الوعي بالمخاطر التي قد تنجم عن اعتراض البيانات أو التجسس الإلكتروني عبر الشبكات العامة، فضلاً عن انتشار النصائح والإرشادات الأمنية المتعلقة باستخدام الإنترنت في الأماكن العامة.

كما تعكس هذه النتيجة امتلاك الطلبة لثقافة أمنية جيدة فيما يتعلق بحماية المعلومات أثناء الاتصال بالشبكات المختلفة، وهو ما يعد مؤشراً إيجابياً على مستوى السلوك الرقمي الآمن لديهم.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (23): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (20)

المحور الرابع: إدراك التهديدات السيبرانية وانعكاساتها

البند رقم (21):

نص البند رقم (21) على: " أدرك أن الأنظمة التقنية للمؤسسات هي الهدف الرئيسي للهجمات السيبرانية الكبرى."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (24) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (21)

البديل	التكرارات	النسبة المئوية
موافق	29	58.0%
محايد	18	36.0%
غير موافق	03	6.0%
الإجمالي	50	100%

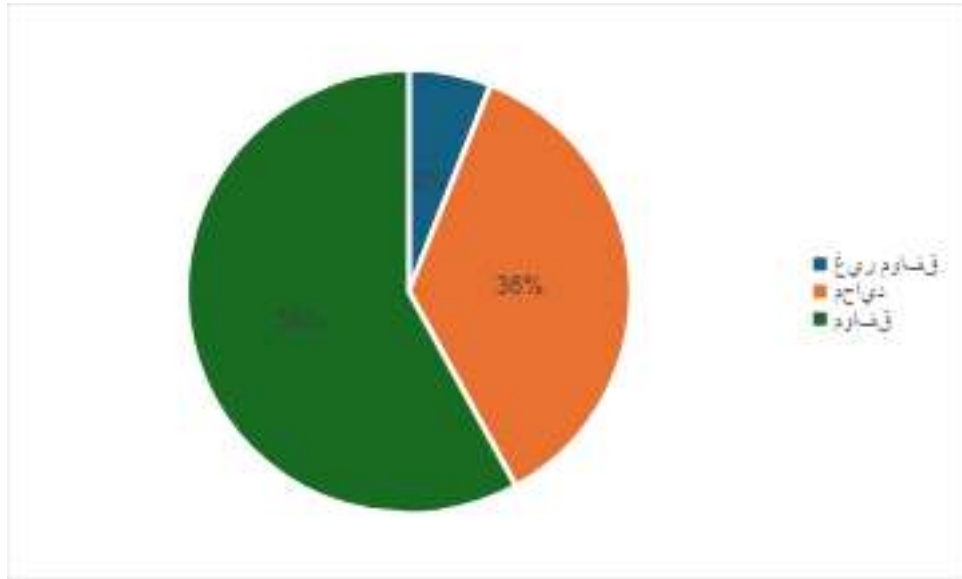
من خلال الجدول أعلاه رقم (24) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (29) فرداً بنسبة مئوية بلغت 58.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجابتهم بالبديل "محايد" والبالغ عددهم (18) فرداً بنسبة 36.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (03) أفراد بنسبة تقدر بـ 6.0%.

تحليل وتفسير :

تشير هذه النتيجة إلى أن أغلبية أفراد العينة يدركون أن المؤسسات بمختلف أنواعها، سواء كانت حكومية أو اقتصادية أو تعليمية، تمثل أهدافاً رئيسية للهجمات السيبرانية نظراً لما تمتلكه من قواعد بيانات ضخمة ومعلومات حساسة ذات قيمة عالية، ويعكس ذلك مستوى جيداً من الوعي بطبيعة التهديدات الرقمية المعاصرة التي أصبحت تستهدف البنى التحتية التقنية للمؤسسات أكثر من استهداف الأفراد بشكل منفرد.

ويمكن تفسير هذه النتيجة بالانتشار الواسع للأخبار المتعلقة بالهجمات الإلكترونية التي تعرضت لها مؤسسات عالمية كبرى، وما ترتب عنها من خسائر مالية وتعطل للخدمات وتسريب للبيانات، كما أن التخصصات التقنية التي ينتمي إليها الطلبة تتيح لهم فهماً أفضل لطبيعة الأنظمة المعلوماتية داخل المؤسسات وأهمية تأمينها.

أما ارتفاع نسبة المحايدين نسبياً فقد يشير إلى أن بعض الطلبة لا يمتلكون تصوراً دقيقاً حول طبيعة الجهات المستهدفة بالهجمات السيبرانية أو يعتقدون أن الأفراد والمؤسسات يتعرضون للمخاطر بنفس الدرجة وهذا ما هو موضح في الشكل التالي:



الشكل رقم (24): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (21)

البند رقم (22):

نص البند رقم (22) على: " ادرك أن خطر الاختراق يهدد سلامة قواعد البيانات الضخمة وأمن المعلومات الحساسة"، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (25) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (22)

البديل	التكرارات	النسبة المئوية
موافق	40	80.0%
محايد	09	18.0%
غير موافق	01	2.0%
الإجمالي	50	100%

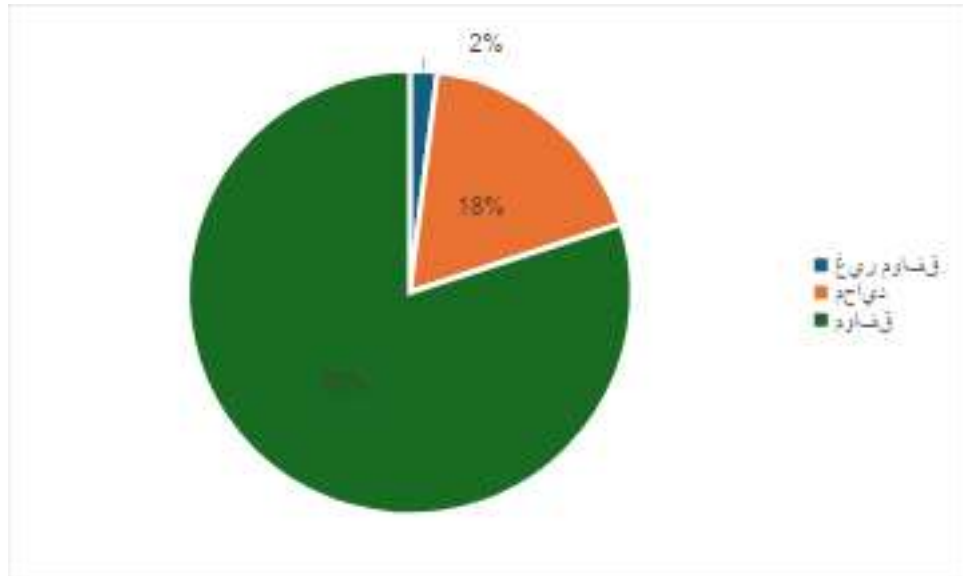
من خلال الجدول أعلاه رقم (25) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (40) فرداً بنسبة مئوية بلغت 80.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (09) أفراد بنسبة 18.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (01) فرد واحد بنسبة مئوية قدرت بـ 2.0%.

تحليل وتفسير:

تعكس هذه النتيجة مستوى مرتفعاً جداً من الوعي لدى الطلبة بخطورة الاختراقات الإلكترونية وتأثيرها المباشر على قواعد البيانات والمعلومات الحساسة، وتدلل هذه النسبة المرتفعة على إدراك أفراد العينة لأهمية البيانات باعتبارها أحد أهم الأصول الرقمية التي تسعى الهجمات السيبرانية إلى استهدافها.

ويمكن تفسير هذه النتيجة بزيادة الاهتمام العالمي بقضايا حماية البيانات الشخصية والمؤسسية، خاصة بعد تكرار حوادث تسريب البيانات التي طالت شركات ومؤسسات كبرى، كما أن الطلبة بحكم تخصصاتهم يدركون الدور المحوري الذي تؤديه قواعد البيانات في تشغيل الأنظمة الرقمية، وأن أي اختراق لها قد يؤدي إلى خسائر تقنية واقتصادية وأمنية كبيرة.

وتؤكد هذه النتيجة نجاح مختلف الجهود التوعوية والإعلامية في ترسيخ مفهوم حماية البيانات باعتباره أحد المرتكزات الأساسية للأمن السيبراني وهذا ما هو موضح في الشكل التالي:



الشكل رقم (25): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (22)

البند رقم (23):

نص البند رقم (23) على: " أدرك أن الهجمات السيبرانية تؤدي إلى تعطيل الخدمات التقنية وفقدان سلامة البيانات في المؤسسات."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (26) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (23)

البديل	التكرارات	النسبة المئوية
موافق	40	80.0%
محايد	07	14.0%
غير موافق	03	6.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (26) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (40) فرداً بنسبة مئوية بلغت 80.0%، أما المجموعة الثانية فتتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (07) أفراد بنسبة 14.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (03) أفراد بنسبة تقدر بـ 6.0%.

تحليل وتفسير:

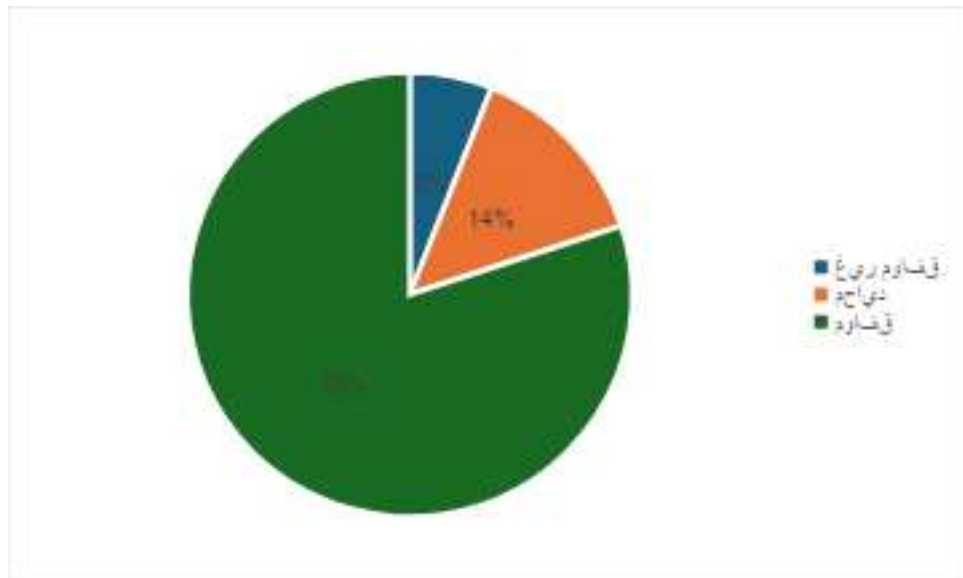
تشير هذه النتيجة إلى أن أغلبية أفراد العينة يدركون الآثار السلبية التي تترتب عن الهجمات السيبرانية على المؤسسات، سواء من خلال تعطيل الخدمات الرقمية أو الإضرار بسلامة البيانات والمعلومات المخزنة داخل الأنظمة.

ويمكن تفسير هذه النتيجة بانتشار المعرفة المتعلقة ببرمجيات الفدية والهجمات التخريبية التي تستهدف الأنظمة المعلوماتية وتسبب في توقف الخدمات الإلكترونية لفترات متفاوتة، إضافة إلى الخسائر المادية والمعنوية

الناجمة عنها، كما أن الطلبة أصبحوا أكثر وعياً بأهمية استمرارية الخدمات الرقمية في المؤسسات الحديثة واعتماد مختلف القطاعات على الأنظمة الإلكترونية في أداء وظائفها.

وتدل هذه النتيجة على أن الطلبة لا يقتصر إدراكهم على معرفة أسباب الهجمات الإلكترونية فحسب، بل يمتد إلى فهم انعكاساتها ونتائجها المحتملة على المؤسسات والمجتمع.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (26): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (23)

البند رقم (24):

نص البند رقم (24) على: " أدرك أن سوء إدارة الوصول إلى الأنظمة والمنصات يفتح ثغرات أمنية للاختراق والتجسس."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (27) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (24)

البديل	التكرارات	النسبة المئوية
موافق	37	74.0%
محايد	10	20.0%
غير موافق	03	6.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (27) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (37) فرداً بنسبة مئوية بلغت 74.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (10) أفراد بنسبة 20.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (03) أفراد بنسبة مئوية قدرت بـ 6.0%.

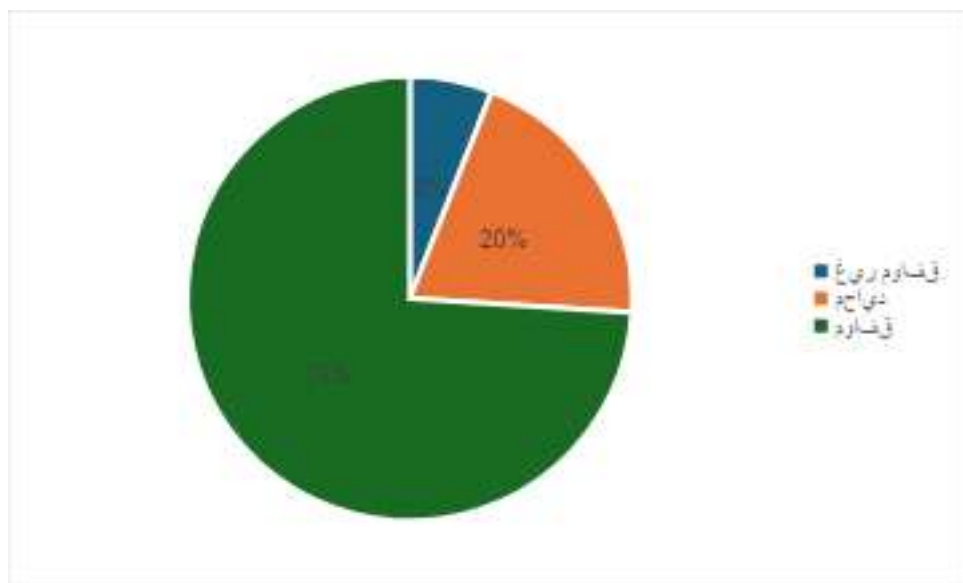
تحليل وتفسير:

تعكس هذه النتيجة إدراكاً مرتفعاً لدى الطلبة لأهمية إدارة الصلاحيات والتحكم في الوصول إلى الأنظمة المعلوماتية باعتبارها من أهم عناصر الحماية الأمنية، ويعني ذلك أن أغلبية أفراد العينة يدركون أن منح صلاحيات غير مناسبة أو ضعف الرقابة على حسابات المستخدمين قد يؤدي إلى استغلال الثغرات الأمنية وتنفيذ عمليات اختراق أو تجسس إلكتروني.

ويمكن تفسير هذه النتيجة بطبيعة التخصصات التقنية التي تركز على مفاهيم إدارة المستخدمين والتحكم في الصلاحيات داخل الأنظمة وقواعد البيانات، فضلاً عن انتشار الوعي بمبدأ "الحد الأدنى من الصلاحيات" الذي يعد من المبادئ الأساسية في الأمن السيبراني.

وتشير هذه النتيجة إلى أن الطلبة يمتلكون فهماً جيداً للعوامل البشرية والتنظيمية التي قد تؤدي إلى حدوث اختراقات أمنية، وليس فقط العوامل التقنية البحتة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (27): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (24)

البند رقم (25):

نص البند رقم (25) على: " أدرك بأن نقص الوعي التقني هو الثغرة الأساسية التي تسهل نجاح الهجمات السيبرانية."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (28) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (25)

البديل	التكرارات	النسبة المئوية
موافق	40	80.0%
محايد	09	18.0%
غير موافق	01	2.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (28) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (40) فرداً بنسبة مئوية بلغت 80.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (09) أفراد بنسبة 18.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (01) فرد واحد بنسبة تقدر بـ 2.0%.

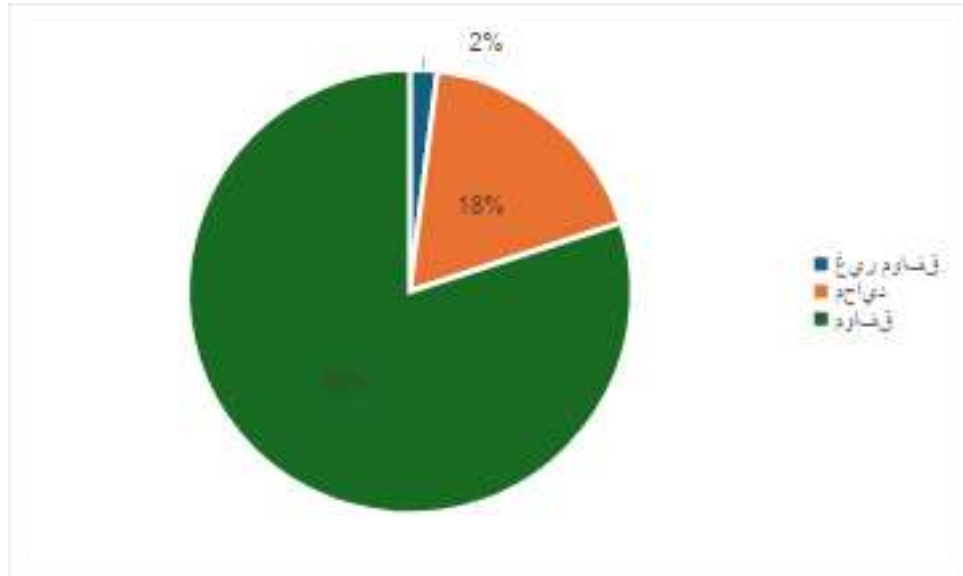
تحليل وتفسير :

تشير هذه النتيجة إلى وجود اتفاق واسع بين أفراد العينة حول أهمية العنصر البشري في منظومة الأمن السيبراني، حيث يرى معظم الطلبة أن نقص الوعي والمعرفة التقنية يمثل أحد أهم الأسباب التي تسهم في نجاح الهجمات الإلكترونية.

ويمكن تفسير هذه النتيجة بأن العديد من الدراسات والتقارير المتخصصة تؤكد أن نسبة كبيرة من الاختراقات تنجح بسبب أخطاء بشرية مثل استخدام كلمات مرور ضعيفة أو فتح روابط مشبوهة أو مشاركة معلومات حساسة دون الانتباه للمخاطر الأمنية، كما أن الطلبة يدركون أن أكثر الأنظمة تطوراً قد تصبح عرضة للاختراق إذا افتقر مستخدميها إلى الوعي الأمني الكافي.

وتبرز هذه النتيجة أهمية التوعية والتدريب المستمر كإحدى الركائز الأساسية لمواجهة التهديدات السيبرانية وتقليل المخاطر الرقمية.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (28): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (25)

البند رقم (26):

نص البند رقم (26) على: " أدرك أن الأخبار الزائفة هي وسيلة لتهديد أمن المعلومات وتضليل المستخدمين."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (29) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (26)

البديل	التكرارات	النسبة المئوية
موافق	34	68.0%
محايد	12	24.0%
غير موافق	04	8.0%
الإجمالي	50	100%

من خلال الجدول أعلاه رقم (29) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (34) فرداً بنسبة مئوية بلغت 68.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (12) فرداً بنسبة 24.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (04) أفراد بنسبة مئوية قدرت بـ 8.0%.

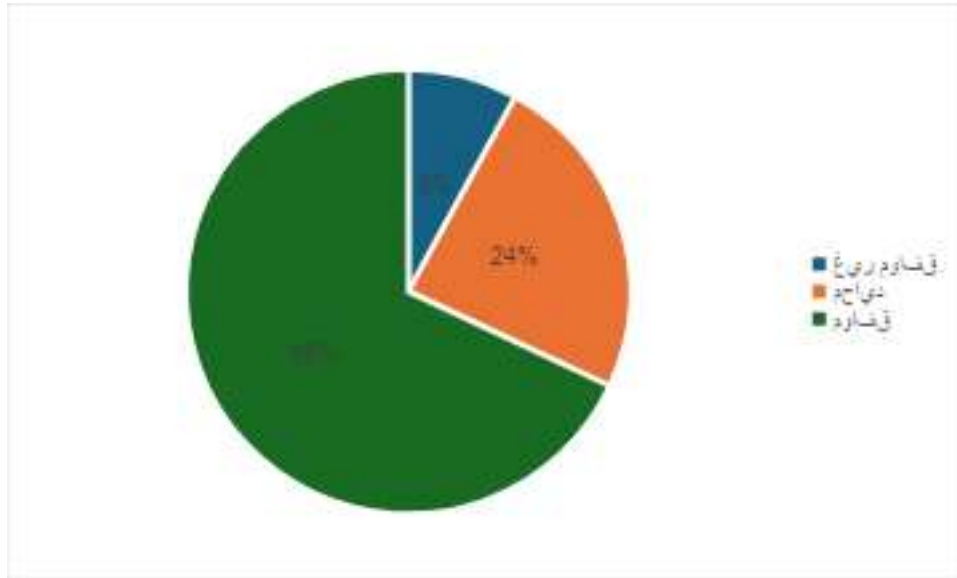
تحليل وتفسير :

تعكس هذه النتيجة وعياً جيداً لدى الطلبة بالعلاقة بين الأخبار الزائفة والأمن السيبراني، حيث يدرك أغلب أفراد العينة أن المعلومات المضللة قد تُستخدم كأداة للتأثير على المستخدمين أو دفعهم إلى اتخاذ قرارات خاطئة قد تعرضهم للمخاطر الأمنية.

ويمكن تفسير هذه النتيجة بالانتشار الواسع للأخبار الكاذبة عبر شبكات التواصل الاجتماعي والمنصات الرقمية، وما يصاحبها من محاولات للتلاعب بالمعلومات أو نشر محتويات مضللة تستهدف الأفراد والمؤسسات، كما أن التطور المتسارع في تقنيات الذكاء الاصطناعي والتزييف الرقمي جعل من الصعب أحياناً التمييز بين المعلومات الصحيحة والمزيفة، مما زاد من أهمية الوعي الإعلامي الرقمي لدى المستخدمين.

وتشير هذه النتيجة إلى أن الطلبة ينظرون إلى الأمن السيبراني من منظور شامل لا يقتصر على الجوانب التقنية فقط، بل يشمل أيضاً الجوانب المعلوماتية والمعرفية المرتبطة بحماية المستخدم من التضليل الرقمي.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (29): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (26)

المحور الخامس: تقييم دور الجامعة وسبل التعزيز

البند رقم (27):

نص البند رقم (27) على: " تفعيل دور الجامعة في نشر ثقافة الأمن السيبراني من خلال برامج توعوية مستمرة."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (30) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (27)

البديل	التكرارات	النسبة المئوية
موافق	32	64.0%
محايد	08	16.0%
غير موافق	10	20.0%
الإجمالي	50	100%

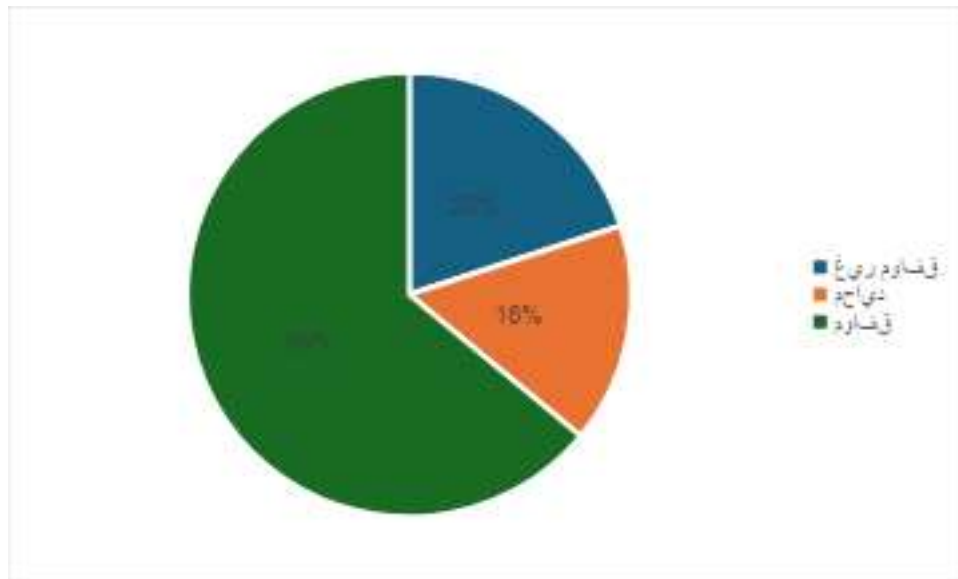
من خلال الجدول أعلاه رقم (30) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (32) فرداً بنسبة مئوية بلغت 64.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (08) أفراد بنسبة 16.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (10) أفراد بنسبة تقدر بـ 20.0%.

تحليل وتفسير :

وتعكس هذه النتيجة إدراك الطلبة لأهمية الدور الذي يمكن أن تؤديه الجامعة في تعزيز الوعي السيبراني من خلال الأنشطة التكوينية والبرامج التوعوية المنتظمة، كما تدل على وجود حاجة فعلية لدى الطلبة للحصول على مزيد من التوجيه والإرشاد في هذا المجال.

وتشير النتيجة كذلك إلى أن بعض الطلبة يرون أن الجهود الحالية ما تزال غير كافية، وهو ما يفسر وجود نسبة من غير الموافقين الذين يطالبون بمزيد من المبادرات التوعوية.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (30) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (27)

البند رقم (28):

نص البند رقم (28) على: " إدراج مقياس الأمن السيبراني كمادة أساسية ضمن المسار الدراسي لمختلف التخصصات."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (31) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (28)

البديل	التكرارات	النسبة المئوية
موافق	33	66.0%
محايد	12	24.0%
غير موافق	05	10.0%
الإجمالي	50	100%

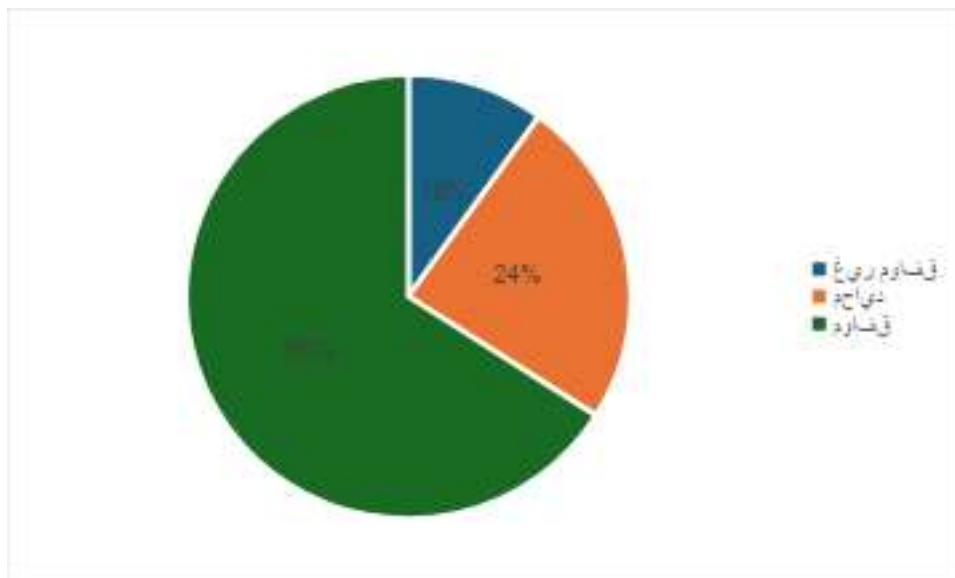
من خلال الجدول أعلاه رقم (31) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (33) فرداً بنسبة مئوية بلغت 66.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (12) فرداً بنسبة 24.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (05) أفراد بنسبة مئوية قدرت بـ 10.0%.

تحليل وتفسير :

وتدل هذه النتيجة على اقتناع أغلبية الطلبة بأن الأمن السيبراني لم يعد مجالاً متخصصاً يقتصر على طلبة الإعلام الآلي فقط، بل أصبح ضرورة لجميع التخصصات الأكاديمية نظراً للاعتماد الواسع على التكنولوجيا الرقمية.

كما تعكس هذه النتيجة وعياً متزايداً بأهمية دمج الثقافة الأمنية الرقمية ضمن التكوين الجامعي بما يساهم في إعداد خريجين قادرين على التعامل الآمن مع التقنيات الحديثة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (31): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (28)

البند رقم (29):

نص البند رقم (29) على: " تنظيم ندوات وملتقيات تقنية دورية لمناقشة طرق الحماية من التهديدات السيبرانية. " ، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (32) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (29)

البديل	التكرارات	النسبة المئوية
موافق	35	70.0%
محايد	07	14.0%
غير موافق	08	16.0%
الإجمالي	50	100%

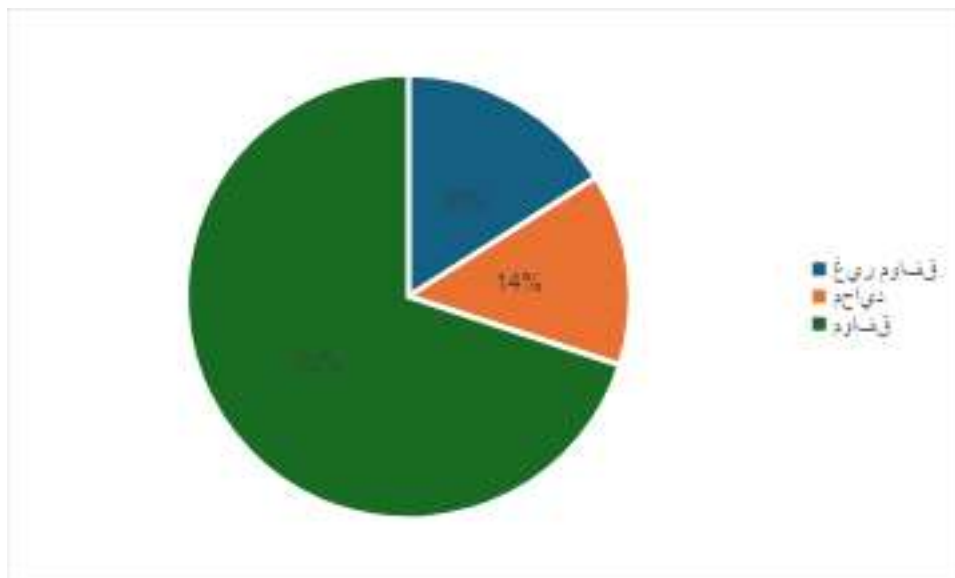
من خلال الجدول أعلاه رقم (32) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (35) فرداً بنسبة مئوية بلغت 70.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (07) أفراد بنسبة 14.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (08) أفراد بنسبة تقدر بـ 16.0%.

تحليل وتفسير :

وتشير هذه النتيجة إلى أن الطلبة ينظرون إلى الندوات والملتقيات العلمية كوسائل فعالة لتطوير معارفهم ومواكبة المستجدات في مجال الأمن السيبراني، خاصة في ظل التطور السريع للتهديدات الرقمية.

كما تعكس رغبة الطلبة في الاستفادة من خبرات المختصين والمهنيين، وربط الجوانب النظرية بالممارسات الواقعية في بيئة العمل التقنية.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (32): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (29)

البند رقم (30):

نص البند رقم (30) على: " توفير ورشات عمل تطبيقية ومخابر متخصصة لتدريب الطلبة على التصدي للاختراقات.", وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (33) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (30)

البديل	التكرارات	النسبة المئوية
موافق	40	80.0%
محايد	10	20.0%
الإجمالي	50	100%
البديل	التكرارات	النسبة المئوية

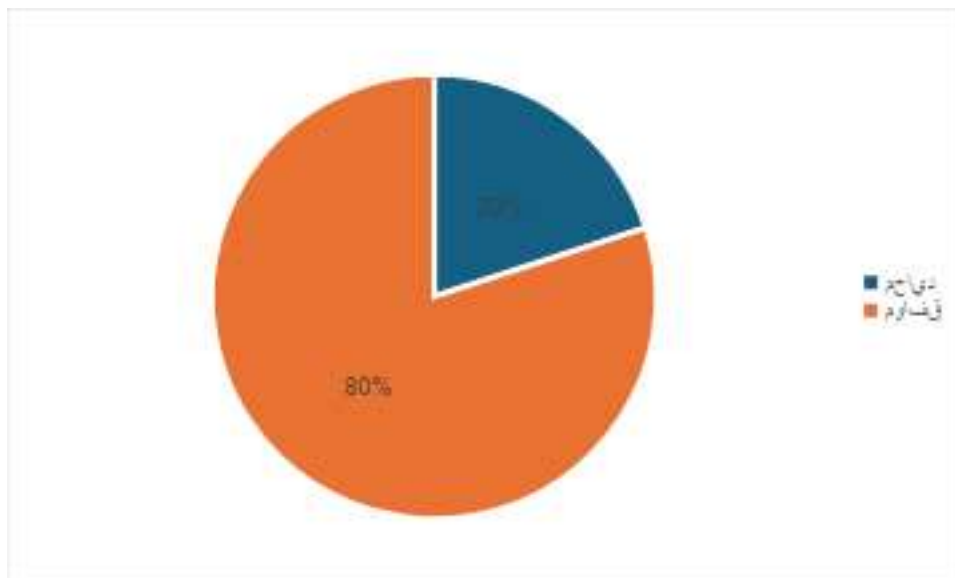
من خلال الجدول أعلاه رقم (33) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى مجموعتين، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (40) فرداً بنسبة مئوية بلغت 80.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (10) أفراد بنسبة 20.0%.

تحليل وتفسير :

وتعد هذه النتيجة من أعلى النسب المسجلة في الاستبيان، ما يدل على اتفاق واسع بين أفراد العينة حول أهمية الجانب التطبيقي في اكتساب المهارات الأمنية، فالطلبة يدركون أن المعرفة النظرية وحدها لا تكفي لفهم طبيعة التهديدات السيبرانية وأساليب مواجهتها.

وتعكس هذه النتيجة الحاجة إلى تعزيز البنية التحتية التدريبية داخل الجامعة من خلال إنشاء مخابر متخصصة ومحاكاة سيناريوهات حقيقية للهجمات الإلكترونية بما يساهم في تطوير الكفاءات العملية للطلبة.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (33): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (30)

البند رقم (31):

نص البند رقم (31) على: " تعزيز الشراكة بين الجامعة والمؤسسات التقنية لتطوير المهارات الأمنية لدى الطلبة."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (34) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (31)

البديل	التكرارات	النسبة المئوية
موافق	33	66.0%
محايد	15	30.0%
غير موافق	02	4.0%
الإجمالي	50	100%

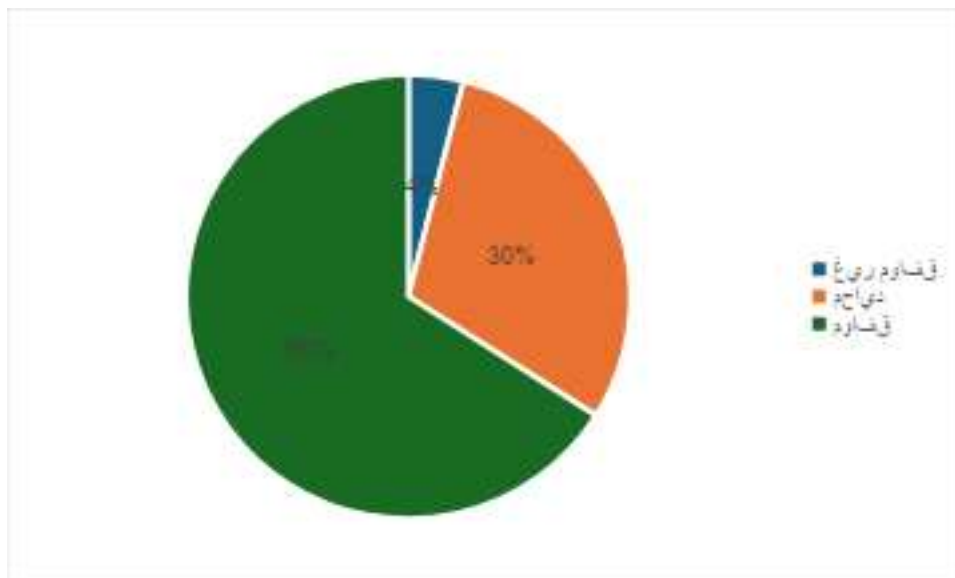
من خلال الجدول أعلاه رقم (34) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (33) فرداً بنسبة مئوية بلغت 66.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (15) فرداً بنسبة 30.0%، في حين تمثلت المجموعة الثالثة في الأفراد الذين كانت إجاباتهم بالبديل "غير موافق" والبالغ عددهم (02) فرد بنسبة مئوية قدرت بـ 4.0%.

تحليل وتفسير

وتشير هذه النتيجة إلى إدراك الطلبة لأهمية التعاون بين الجامعة والقطاع المهني في مجال الأمن السيبراني، حيث تتيح هذه الشراكات فرصاً للتدريب الميداني ونقل الخبرات العملية وتطوير المهارات التقنية المطلوبة في سوق العمل.

كما تعكس النتيجة وعياً متزايداً بأهمية الربط بين الجانب الأكاديمي والجانب التطبيقي بما يضمن تكويناً أكثر ملاءمة لمتطلبات التحول الرقمي.

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (34): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (31)

البند رقم (32):

نص البند رقم (32) على: " تكثيف الحملات الرقمية التوعوية حول الاستخدام الآمن للأنظمة والبيانات الجامعية."، وبعد المعالجة الإحصائية تم التوصل إلى النتيجة الموضحة في الجدول التالي:

الجدول رقم (35) يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (32)

البديل	التكرارات	النسبة المئوية
موافق	38	76.0%
محايد	07	14.0%
غير موافق	05	10.0%
الإجمالي	50	100%

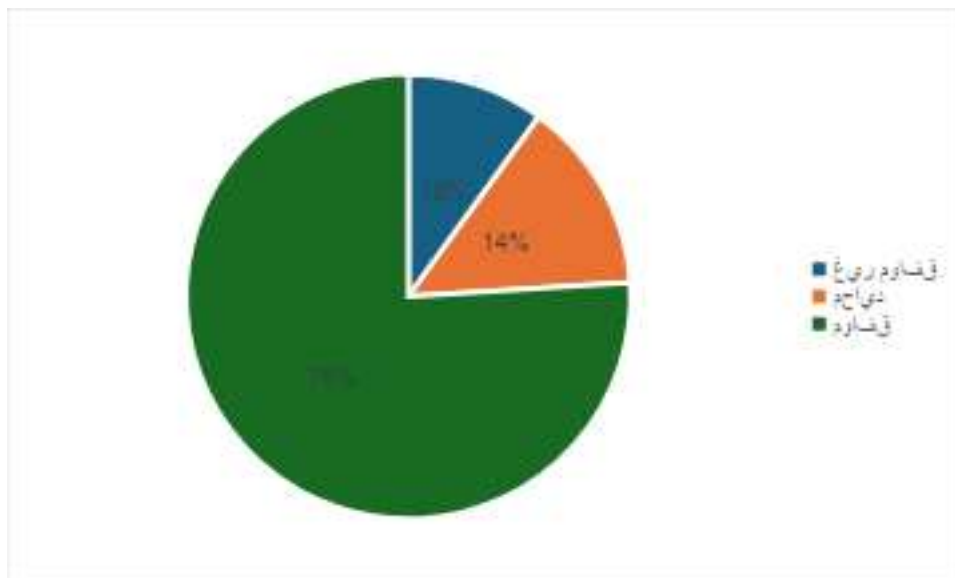
من خلال الجدول أعلاه رقم (35) نلاحظ أن إجابات أفراد عينة الدراسة والبالغ عددهم إجمالاً (50) فرداً قد انقسمت إلى ثلاث مجموعات، تمثلت المجموعة الأولى في الأفراد الذين تمحورت إجاباتهم بالبديل "موافق" وقد بلغ عددهم (38) فرداً بنسبة مئوية بلغت 76.0%، أما المجموعة الثانية فتمثل الأفراد الذين كانت إجاباتهم بالبديل "محايد" والبالغ عددهم (07) أفراد بنسبة 14.0%، بينما المجموعة الثالثة تمثلت في الأفراد الذين اختاروا البديل "غير موافق" وعددهم (05) أفراد بنسبة تقدر بـ 10.0%.

تحليل وتفسير :

وتدل هذه النتيجة على اقتناع أغلبية الطلبة بأهمية الحملات التوعوية الرقمية كوسيلة فعالة لنشر ثقافة الأمن السيبراني داخل الوسط الجامعي، كما تعكس إدراكهم بأن الوقاية من المخاطر الإلكترونية تبدأ من نشر المعرفة الصحيحة وتطوير السلوكيات الرقمية الآمنة.

ويمكن تفسير هذه النتيجة بزيادة الاعتماد على المنصات الرقمية في الدراسة والتواصل الجامعي، الأمر الذي يجعل من التوعية المستمرة ضرورة أساسية للحفاظ على أمن المعلومات والأنظمة الرقمية داخل الجامعة

وهذا ما هو موضح في الشكل التالي:



الشكل رقم (35): يوضح توزيع إجابات أفراد عينة الدراسة على البند رقم (32)

ثانيا/ الجداول المركبة

الجدول رقم (36) إجابات أفراد عينة الدراسة على البند رقم (1) حسب الجنس

النسبة		البند رقم (01) تبعا للجنس			
		موافق	محايد	غير موافق	
	المجموع				
64%	32	23	6	3	ذكر
36%	18	9	3	6	أنثى
100%	50	32	9	9	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 5 والمتعلق بـ "لدي معرفة بعض المفاهيم الأساسية للأمن السيبراني، مثل التشفير وحماية البيانات." حسب الجنس، نلاحظ أن أغلب أفراد العينة كانت إجاباتهم في خانة "غير موافق"، حيث بلغ عددهم (32) فردا بنسبة (64%) من إجمالي العينة، منهم (23) ذكرا و(9) إناث، مما يدل على ضعف مستوى المعرفة بالمفاهيم الأساسية للأمن السيبراني لدى أغلب أفراد الدراسة.

كما بلغت نسبة الموافقين (9) أفراد بنسبة (18%)، موزعين بين (3) ذكور و(6) إناث، في حين بلغت فئة "محايد" أيضا (9) أفراد بنسبة (18%). وتشير هذه النتائج إلى محدودية التكوين المعرفي لدى الطلبة في مجال الأمن السيبراني، رغم وجود بعض الفروق البسيطة بين الجنسين لصالح الإناث في فئة الموافقة.

الجدول رقم (37) إجابات أفراد عينة الدراسة على البند رقم (02) حسب الجنس

النسبة		البند رقم (02) تبعا للجنس			
		موافق	محايد	غير موافق	
	الجموع				
64%	32	23	6	3	ذكر
36%	18	14	2	2	أنثى
100%	50	37	8	5	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 5 والمتعلق بـ "أدرك المخاطر التقنية المرتبطة بالتعامل مع الشبكات المفتوحة ومنصات تبادل البيانات." حسب الجنس، نلاحظ أن أغلبية أفراد العينة اختاروا "غير موافق"، حيث بلغ عددهم (37) فردا بنسبة (74%)، منهم (23) ذكرا و(14) أنثى، وهو ما يعكس انخفاض مستوى إدراك المخاطر التقنية المرتبطة باستخدام الشبكات المفتوحة ومنصات تبادل البيانات.

كما بلغت فئة "محايد" (8) أفراد بنسبة (16%)، بينما لم تتجاوز فئة "موافق" (5) أفراد بنسبة (10%)، مما يشير إلى ضعف الوعي بالمخاطر الرقمية لدى أفراد العينة، وهو ما قد يرجع إلى نقص التكوين أو محدودية الثقافة السيبرانية لديهم.

الجدول رقم (38) إجابات أفراد عينة الدراسة على البند رقم (05) حسب الجنس

النسبة		البند رقم (05) تبعا للجنس			
		موافق	محايد	غير موافق	
	الجموع				
64%	32	21	8	3	ذكر
36%	18	13	5	0	أنثى
100%	50	34	13	3	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 5 والمتعلق بـ "أعرف أهمية تطبيق إجراءات الأمن السيبراني أثناء استخدام الأنظمة الإلكترونية؟" حسب الجنس، نلاحظ أن أغلب أفراد العينة كانت إجاباتهم في خانة "غير موافق"، حيث بلغ عددهم (34) فردا بنسبة (68%)، منهم (21) ذكرا و(13) أنثى، وهو ما يدل على ضعف الوعي بأهمية تطبيق إجراءات الأمن السيبراني أثناء استخدام الأنظمة الإلكترونية.

كما سجلت فئة "محايد" (13) فردا بنسبة (26%)، بينما بلغت فئة "موافق" (3) أفراد فقط بنسبة (6%)، وجميعهم من الذكور. وتبين هذه النتائج أن إدراك أهمية تطبيق الإجراءات الوقائية الرقمية ما يزال محدودا لدى الطلبة، الأمر الذي يستدعي تعزيز التوعية والتكوين في هذا المجال.

الجدول رقم (39) إجابات أفراد عينة الدراسة على البند رقم (08) حسب الجنس

النسبة		البند رقم (08) تبعا للجنس			
		موافق	محايد	غير موافق	
	الاجموع				
64%	13	16	3	13	ذكر
36%	4	11	3	4	أنثى
100%	17	27	6	17	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 8 والمتعلق بـ "يساهم التكوين الجامعي في تعزيز وعيي بأسس الأمن السيبراني" حسب الجنس، نلاحظ أن أغلب أفراد العينة كانت إجاباتهم في خانة "غير موافق"، حيث بلغ عددهم (27) فردا بنسبة (54%)، منهم (16) ذكرا و(11) أنثى، مما يشير إلى أن التكوين الجامعي لا يساهم بالشكل الكافي في تعزيز وعي الطلبة بأسس الأمن السيبراني.

في المقابل بلغت فئة "موافق" (17) فردا بنسبة (34%)، موزعين بين (13) ذكرا و(4) إناث، بينما بلغت فئة "محايد" (6) أفراد بنسبة (12%). وتشير هذه النتائج إلى وجود قصور نسبي في إدماج موضوعات الأمن السيبراني ضمن التكوين الجامعي أو ضعف الجانب التطبيقي المرتبط به.

الجدول رقم (40) إجابات أفراد عينة الدراسة على البند رقم (13) حسب الجنس

النسبة		البند رقم (13) تبعا للجنس			
		موافق	محايد	غير موافق	
	المجموع				
64%	32	12	7	13	ذكر
36%	18	5	6	7	أنثى
100%	50	17	13	20	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 13 والمتعلق بـ "أكتسب مهارات حماية الأنظمة والبيانات من خلال التطبيق العملي في المخابر الجامعية والتدريبات التقنية المتخصصة" حسب الجنس، نلاحظ أن هناك تقاربا نسبيا بين إجابات أفراد العينة، حيث بلغت فئة "موافق" (20) فردا بنسبة (40%)، منهم (13) ذكرا و(7) إناث، بينما بلغت فئة "غير موافق" (17) فردا بنسبة (34%).

كما بلغت فئة "محايد" (13) فردا بنسبة (26%). وتدلل هذه النتائج على أن جزءا معتبرا من الطلبة يرى أن المخابر الجامعية والتدريبات التطبيقية تساعدهم على اكتساب بعض مهارات الحماية الرقمية، إلا أن نسبة غير الموافقين تشير في المقابل إلى وجود حاجة لتعزيز الجانب التطبيقي والتقني في التكوين الجامعي.

الجدول رقم (41) إجابات أفراد عينة الدراسة على البند رقم (15) حسب الجنس

النسبة		البند رقم (15) تبعا للجنس			
		موافق	محايد	غير موافق	
	المجموع				
64%	32	18	11	3	ذكر
36%	18	10	6	2	أنثى
100%	50	28	17	5	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند

رقم 15 والمتعلق بـ "أجنب مشاركة بيانات الاعتماد (Credentials) أو الأكواد البرمجية الخاصة عبر المنصات غير المشفرة" حسب الجنس، نلاحظ أن أغلب أفراد العينة كانت إجاباتهم في خانة "غير موافق"،

حيث بلغ عددهم (28) فردا بنسبة (56%)، منهم (18) ذكرا و(10) إناث، وهو ما يعكس ضعف الالتزام بالممارسات الآمنة المرتبطة بحماية البيانات وبيانات الاعتماد.

كما بلغت فئة "محايد" (17) فردا بنسبة (34%)، بينما بلغت فئة "موافق" (5) أفراد فقط بنسبة (10%). وتشير هذه النتائج إلى محدودية الوعي بالمخاطر المرتبطة بمشاركة البيانات الحساسة عبر المنصات غير الآمنة.

الجدول رقم (42) إجابات أفراد عينة الدراسة على البند رقم (18) حسب الجنس

النسبة		البند رقم (18) تبعا للجنس			
		موافق	محايد	غير موافق	
	الاجموع				
64%	32	19	8	5	ذكر
36%	18	10	5	3	أنثى
100%	50	24	18	8	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 18 والمتعلق بـ "الترزم بتطبيق مبادئ الأمن منذ التصميم (Dzsigne by Security) عند بناء النظم البرمجية، مع التركيز على تأمين واجهات البرمجة (APIs) ومن تسرب البيانات" حسب الجنس، نلاحظ أن أغلب أفراد العينة كانت إجاباتهم في خانة "غير موافق"، حيث بلغ عددهم (24) فردا بنسبة (48%)، منهم (19) ذكرا و(5) إناث.

كما بلغت فئة "محايد" (18) فردا بنسبة (36%)، في حين بلغت فئة "موافق" (8) أفراد بنسبة (16%). وتوضح هذه النتائج أن أغلب الطلبة لا يمتلكون وعيا كافيا بمبادئ الأمن السيبراني المرتبطة بتطوير الأنظمة وتأمين البيانات، وهو ما قد يعكس نقص التكوين التقني المتخصص في هذا المجال.

الجدول رقم (43) إجابات أفراد عينة الدراسة على البند رقم (21) حسب الجنس

النسبة		البند رقم (21) تبعا للجنس			
		موافق	محايد	غير موافق	
	المجموع				
64%	32	5	8	19	ذكر
36%	18	3	10	5	أنثى
100%	50	8	18	24	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 21 والمتعلق بـ "أدرك أن الأنظمة التقنية للمؤسسات هي الهدف الرئيسي للهجمات السيبرانية الكبرى" حسب الجنس، نلاحظ أن فئة "غير موافق" جاءت في المرتبة الأولى بـ (24) فردا بنسبة (48%)، يليها "محايد" بـ (18) فردا بنسبة (36%)، ثم "موافق" بـ (8) أفراد بنسبة (16%).

وتشير هذه النتائج إلى أن مستوى إدراك الطلبة لطبيعة الهجمات السيبرانية والأهداف التي تستهدفها ما يزال متوسطا إلى ضعيفا، الأمر الذي يعكس الحاجة إلى تنمية الثقافة التقنية والأمنية لدى الطلبة بشكل أكبر.

الجدول رقم (44) إجابات أفراد عينة الدراسة على البند رقم (25) حسب الجنس

النسبة		البند رقم (25) تبعا للجنس			
		موافق	محايد	غير موافق	
	المجموع				
64%	32	0	7	25	ذكر
36%	18	1	2	15	أنثى
100%	50	1	9	40	الإجمالي

من خلال الجدول أعلاه وبالنظر إلى إجابات أفراد عينة الدراسة على البند رقم 25 والمتعلق بـ "أدرك بأن نقص الوعي التقني هو الثغرة الأساسية التي تسهل نجاح الهجمات السيبرانية" حسب الجنس، نلاحظ أن أغلبية كبيرة

من أفراد العينة اختارت "غير موافق"، حيث بلغ عددهم (40) فردا بنسبة (80%)، منهم (25) ذكرا و(15) أنثى، وهي أعلى نسبة ضمن جميع الأسئلة السابقة.

كما بلغت فئة "محايد" (9) أفراد بنسبة (18%)، في حين سجلت فئة "موافق" فردا واحدا فقط بنسبة (2%).
وتدل هذه النتائج على انخفاض واضح في إدراك أفراد العينة لأهمية الوعي التقني ودوره الأساسي في الوقاية من الهجمات السيبرانية، مما يؤكد الحاجة الملحة إلى تعزيز الثقافة الرقمية والأمنية لدى الطلبة من خلال برامج تكوينية وتوعوية متخصصة.

الاستنتاج العام للدراسة:

من خلال النتائج المتوصل إليها في دراستنا، يتبين أن طلبة الإعلام الآلي بجامعة المسيلة يتمتعون بمستوى جيد من المعرفة والوعي بالأمن السيبراني، حيث أظهروا إدراكاً واضحاً للمفاهيم الأساسية المرتبطة بحماية البيانات والمعلومات الرقمية، إضافة إلى وعي معتبر بالمخاطر والتهديدات السيبرانية المعاصرة.

كما بينت النتائج أن الطلبة يعتمدون على مصادر متنوعة لاكتساب معارفهم في هذا المجال، تصدرها المنصات التقنية والمواقع المتخصصة والمراجع العلمية، في حين أظهرت بعض المؤشرات وجود حاجة إلى تعزيز دور الجامعة في توفير التكوين العملي والتطبيقي المرتبط بالأمن السيبراني.

وقد كشفت الدراسة أيضاً عن تبني أغلبية الطلبة لعدد من السلوكيات الرقمية الآمنة، مثل استخدام وسائل الحماية المختلفة وتحديث الأنظمة والتحقق من صلاحيات التطبيقات والحرص على حماية البيانات الشخصية.

كما أظهرت النتائج وجود اتفاق كبير بين أفراد العينة حول أهمية تطوير البرامج الجامعية المتعلقة بالأمن السيبراني من خلال إدراج مقاييس متخصصة، وتنظيم دورات تدريبية وورشات تطبيقية، وتعزيز الشراكات مع المؤسسات التقنية، وتكثيف الحملات التوعوية الرقمية.

وعليه يمكن القول أن مستوى الوعي بالأمن السيبراني لدى الطلبة محل الدراسة يعد إيجابياً بصفة عامة، غير أن تعزيز الجانب التطبيقي والتكويني داخل الجامعة يبقى ضرورة أساسية لمواكبة التطورات المتسارعة في مجال التهديدات السيبرانية وضمان إعداد كفاءات قادرة على التعامل مع التحديات الأمنية الرقمية المستقبلية.

مناقشة النتائج على ضوء التساؤلات والدراسات السابقة :

في إطار الاجابة عن تساؤلات دراسة حول مستوى الوعي بالأمن السيبراني لدى طلبة الإعلام الآلي بجامعة محمد بوضياف بالمسيلة، ومقارنةً بالدراسات السابقة فيما يتعلق بمستوى معرفة الطلبة بمفاهيم ومخاطر الأمن السيبراني أظهرت نتائجنا الميدانية أن الطلبة يتمتعون بمستوى جيد من المعرفة وإدراك واضح للتهديدات وهو ما يشكل تبايناً مع نتائج دراسة برادة ودحماني (2024) ودراسة سمير عزيزي ويوسف الصديق سلامة (2025) التي انتهتا إلى أن مستوى الوعي كان متوسطاً ويرجع هذا الاختلاف إلى الطابع التخصصي لطلبة الإعلام الآلي الذي منحهم تفوقاً معرفياً.

أما بخصوص الممارسات والسلوكيات الرقمية ومصادر الوعي فقد كشفت نتائجنا أن الطلبة يتبنون سلوكيات آمنة كالتحقق من الصلاحيات وتحديث الأنظمة، وهي نتيجة متطورة مقارنة بما رصدته دراسة ثابت مصطفى وآخرون (2022) من ضعف في إجراءات الحماية الفعلية مما يشير إلى تحسن نوعي في الممارسات الرقمية الحالية وفيما يخص تقييم الطلبة لدور الجامعة، فقد أكدت نتائجنا وجود فجوة تستوجب تعزيز الجانب التطبيقي وهو ما يتطابق مع ما دعت إليه دراسة محمد شريف بكور (2025) ودراسة موسى وآخرون (2025) بضرورة دعم التكوين الأكاديمي بورشات تدريبية، ومع ما أشارت إليه دراسة رباب طاهر محي (2023) حول أهمية نشر الوعي السيبراني

يستنتج من مجمل هذا التحليل الميداني أن طلبة الإعلام الآلي بجامعة المسيلة يمتلكون قاعدة معرفية وسلوكية صلبة حيث أظهروا إدراكاً واضحاً بأن نقص الوعي التقني يمثل ثغرة تسهل الهجمات السيبرانية.

وبذلك، فإن نتائج الدراسة تؤكد أن عينة الطلبة تجاوزت حدود الوعي المتوسط لتصل إلى مستوى من الممارسة الرقمية الواعية مما يجعلهم أكثر قدرة على مواجهة التحديات السيبرانية الفعلية في بيئتهم الرقمية.

الخاتمة

خاتمة :

في ختام الدراسة، نستخلص أن التطورات التكنولوجية المتسارعة فرضت تحديات أمنية حقيقية أعادت تشكيل مفهوم الوعي السيبراني لدى طلبة الجامعة الذين وجدوا أنفسهم أمام ضرورة الانتقال من الاعتماد على المعارف النظرية التقليدية إلى توظيف المهارات الرقمية في حماية أمنهم المعلوماتي مواكباً بذلك لمتطلبات الجيل الحالي الذي يقضي معظم وقته في الفضاء الرقمي.

ومن هنا، تبرز الحاجة لتبني ممارسات رقمية تفاعلية تتجاوز الأساليب الكلاسيكية وتجعل من الطالب عنصراً فعالاً يدرك كيفية حماية خصوصيته وبياناته وليس مجرد مستخدم للأدوات التقنية ليتحول استغلال طاقات الطلبة وتوجيهها ضمن بنية تكوينية منظمة إلى ممارسات ميدانية فعلية ، مما يرفع من كفاءة الأمن السيبراني داخل الحرم الجامعي ويضمن بناء "مناعة رقمية" ذاتية تحصن عقول الطلبة كخط دفاع ضد أي تهديدات أو اختراقات الكترونية .

يعكس هذا التوجه أهمية اعتماد استراتيجيات دفاعية استباقية تتماشى مع طبيعة الفضاء الرقمي المتغير مما يجعل المؤسسة الجامعية بيئة حاضنة للابتكار الأمني، قادرة على دمج البحث العلمي بالواقع العملي وأكثر مرونة وقدرة على التكيف مع التحديات المستجدة.

وبناءً على ما توصلت إليه الدراسة من نتائج وتحليلات ميدانية ، يمكن تقديم مجموعة من التوصيات العملية الموجهة لمختلف الأطراف المعنية بالأمن السيبراني داخل الوسط الجامعي، والمتمثلة فيما يلي :

1. إطلاق نوادي رقمية تخصصية للأمن السيبراني في كل كلية، تكون مفتوحة لجميع التخصصات وتدار من طرف الطلبة تحت إشراف أساتذة، مع إدراج مفاهيم السلامة الرقمية ضمن المقررات الدراسية لضمان وصولها لأكبر عدد من الطلبة.

2. اعتماد "سياسة رقمية آمنة " تركز على توزيع محتوى توعوي دوري يتضمن أدوات وبرامج حماية، والتحول نحو المعالجة التقنية الاستباقية للثغرات البرمجية بدلاً من الاكتفاء بالجانب النظري مع تنظيم ورشات تدريبية مستمرة تعزز ثقة الطلبة في التعامل مع المنظومات الرقمية.

3. تفعيل الرقابة التقنية للأنظمة الجامعية، وإطلاق "رزانة تدريب سيبراني" موزعة على مدار السنة الدراسية لضمان استمرارية التكوين وتجنب ضياع المعلومة التي قد تحدث عند الاقتصار على أيام تكوينية محدودة.

4. إنشاء لجان استشارية علمية دائمة لمراجعة أمن الأنظمة الجامعية مع استضافة خبراء تقنيين متخصصين عبر منصات التدريب عن بعد وبناء شراكات مع المؤسسات المختصة لربط العمق الأكاديمي للجامعة بالتجربة الميدانية الواقعية.

إن تطبيق هذه التوصيات يتطلب تضافر جهود الإدارة، والأساتذة، والطلبة من مختلف التخصصات لضمان استمرارية هذا الوعي وتحويله إلى سلوك يومي يعزز من صمود منظومتنا الرقمية الجامعية أمام التحديات الراهنة والمستقبلية.

قائمة العراجع

قائمة المصادر والمراجع :

أولاً: الكتب

1. عوفي مصطفى. أمن المعلومات والخصوصية الرقمية. عمان: دار اليازوري العلمية، 2022.
2. علاء عبد الخالق حسين وآخرون. الأمن السيبراني المبادئ والممارسات لضمان سلامة المعلومات. بغداد: دار السرد للطباعة والنشر والتوزيع، 2024.
3. رمضاني مراد. التثقيف والتوعية بالأمن السيبراني. وهران: دار العيون للنشر الإلكتروني، 2025.
4. صادق عباس مصطفى. تطبيقات الإعلام الرقمي والاندماج التكنولوجي: الرؤى والآفاق. دار الفكر العربي للنشر والتوزيع، 2024.
5. محمد عبد الفتاح. سوسيولوجيا الشباب الجامعي في العصر الرقمي. المكتب الجامعي الحديث، 2021.
6. مصطفى محمد منجود. الأبعاد السياسية لمفهوم الأمن في الإسلام. القاهرة: المعهد العالمي للفكر الإسلامي، 1996.

ثانياً: المعاجم

1. ابن منظور، محمد بن مكرم. لسان العرب. ط3، بيروت: دار صادر، 1414هـ، مجلد 15.
2. معجم المعاني الجامع. "انتهاك"، مادة لغوية. الرابط:
<https://www.almaany.com/ar/dict/ar-ar/انتهاك>.

ثالثاً: المجلات العلمية

1. برادة عبد الرزاق، ودحماني، فاطمة. "مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية لدى مستخدمي الإنترنت في الجزائر". مجلة البحوث والدراسات الإعلامية، جامعة الجزائر، 2024.
2. ثابت مصطفى، وبوعكاز، حدة، وربوح، عبلة. "وعي الطالب الجامعي بالأمن السيبراني ومخاطر انتهاك الخصوصية". مجلة الاتصال والمجتمع، جامعة ورقلة، 2022.
3. عزيزي سمير، وسلامة، يوسف الصديق. "الوعي بالأمن السيبراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال". المجلة الجزائرية لبحوث الاتصال، جامعة الوادي، 2025.

4. موسى مروة، وآخرون. "دور الوعي بالأمن السيبراني في عصر التحول الرقمي". مجلة التنمية والتحول الرقمي، 2025.
5. سيناء علي محمود. "التحديات الأمنية للدول في الفضاء السيبراني". مجلة قضايا سياسية، جامعة النهدين، 2024.
6. إيهاب خليفة. "الأمن السيبراني: الماهية والإشكاليات". مجلة رؤى مصرية، 2019.
7. محمد مصطفى محمد حمد وآخرون. "دور الأمن السيبراني في مواجهة المخاطر الإلكترونية". المجلة العلمية لكلية التربية جامعة أسيوط، 2024.
8. جيهان سعد محمد الحضري وآخرون. "الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية". مجلة تطوير الأداء الجامعي، 2020.
9. سناء أحمد عبد الله الشديفات. "الأمن السيبراني وحماية البيانات في أقسام بلدية منشية بني حسن". مجلة العلوم الإنسانية والطبيعية (HNSJ)، 2024.
10. منى عبد الله السمحان. "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية". مجلة كلية التربية، 2020.
11. الحسيني فايزة. "الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلومات". مجلة Recherche، 2023.
12. أحمد حاتم جبار عطية. "الأبعاد القانونية والاجتماعية للأمن السيبراني". مجلة الشرق الأوسط للدراسات القانونية والفقهية، 2025.
13. حسية لولي. "الشباب ومظاهر التغير في ظل العولمة". دراسات اجتماعية، العدد 18.
14. أحمد مصطفى محمد أحمد القوصي. "فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني". مجلة الإرشاد النفسي، 2024.

رابعاً: الأطروحات والمذكرات (الرسائل الجامعية)

1. عبد الرزاق، برادة. "مستوى الوعي السيبراني في الوسط الجامعي الجزائري وعلاقته بالجريمة الإلكترونية". أطروحة دكتوراه، جامعة غليزان، 2024.
2. العربي، بن حمار صدام، ورفاع، محمد. "شبكات التواصل الاجتماعي وأثرها على القيم الدينية لدى الطلبة الجامعيين". مذكرة ماستر، جامعة عبد الحميد بن باديس، 2015.

3. عوالمية، إكرام وآخرون. "الثقة بالنفس وعلاقتها بالتوجه نحو الحياة لدى الشباب الجامعي". مذكرة ماستر، جامعة 8 ماي 1945 قالمة، 2025.
4. عباس، آمنة، وخلف الله، رانية. "وعي الطلبة الجامعيين الجزائريين بمخاطر انتهاك الخصوصية". مذكرة ماستر، جامعة 8 ماي 1945 قالمة، 2023.

خامساً: الوثائق والتقارير

1. الجمهورية الجزائرية. القانون رقم 04-18 المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، 2018.
2. الاتحاد الدولي للاتصالات. تقرير اتجاهات الإصلاح في الاتصالات، 2010-2011.

سادساً: المراجع باللغة الأجنبية

1. Cisco Networking Academy. Introduction to Cyber Security Course, 2021
2. Jason R. C. Nurse. "Cybersecurity Awareness". University of Kent, 2022
3. Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology". MIS Quarterly, 13(3), 319–340
4. Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change". The Journal of Psychology, 91(1), 93–114
5. Rogers, R. W., & Prentice-Dunn, S. (1997). "Protection motivation theory". In D. S. Gochman (Ed.), Handbook of health behavior research I: Personal and social determinants (pp. 113–132). Plenum Press

سابعاً: المواقع الإلكترونية

1. إيرث، ماريا، وكيمبرلي وينستون. "انتهاك الخصوصية". الموقع: <https://study.com>
2. جميل، حسين طويلة. "تاريخ الأمن السيبراني". الموقع: <https://www.cyberpedia.site>
3. محمود، الخطيب. "ما هي تطبيقات الإعلام الرقمي؟". الموقع: <https://tawasulforum.org>

الملاحق



جامعة محمد بوضياف - المسيلة -

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

تخصص: اتصال وعلاقات عامة

الموضوع : تعبئة استبيان لإنجاز مذكرة ماستر

في إطار إنجازنا لمذكرة لنيل شهادة الماستر أكاديمي في تخصص اتصال وعلاقات عامة تحت عنوان: " مستوى الوعي بالأمن السيبراني لدى طلبة الإعلام الالي بجامعة محمد بوضياف المسيلة "، نحن بصدد تطبيق استمارة استبيان للحصول على المعلومات اللازمة لإنجاز البحث، لذا يرجى من سيادتكم المحترمة التكرم بالإجابة على أسئلة الاستبيان آمليين منكم توخي الدقة والموضوعية والشفافية لما له من أثر ايجابي في إنجاح هذا البحث، وذلك بوضع علامة (X) في الخانة التي تمثل وجهة نظركم نحو كل عبارة من العبارات الواردة في الاستبيان علما بأن المعلومات الواردة في هذا الاستبيان ستستخدم لأغراض البحث العلمي فقط.

تقبلوا منا فائق الاحترام...

إشراف الدكتور:

- د/ فقيري ليلي

إعداد الطلبة:

- مروة ولهة
- بشيري شيماء



القسم الأول: البيانات الشخصية

يرجى وضع علامة (✓) أمام الإجابة المناسبة:

1-الجنس:

• ذكر ☐

• أنثى ☐

2-العمر:

• من 21 إلى 23 سنة ☐

• من 24 إلى 26 سنة ☐

• أكثر من 26 سنة ☐

3-التخصص :

• ذكاء اصطناعي (IA) ☐

• هندسة البرمجيات ونظم المعلومات (SI /GL) ☐

4-هل تعرضت سابقاً لأي نوع من أنواع التهديد أو الاختراق الرقمي؟

• نعم ☐

• لا ☐

المحور الأول: مستوى المعرفة بالأمن السيبراني				
الرقم	العبارة	موافق	محايد	غير موافق
1	لدي معرفة ببعض المفاهيم الأساسية للأمن السيبراني، مثل التشفير وحماية البيانات.			
2	أدرك المخاطر التقنية المرتبطة بالتعامل مع الشبكات المفتوحة ومنصات تبادل البيانات.			
3	أتابع المنصات الأكاديمية والمواقع التقنية المتخصصة للاطلاع على المستجدات المتعلقة بالأمن السيبراني .			
4	أعرف أهمية تطبيق إجراءات الأمن السيبراني أثناء استخدام الأنظمة الإلكترونية.			
5	أمتلك مهارة التعامل مع إعدادات الأمان المتقدمة لضمان سلامة البيانات الرقمية.			

الملاحق

			أدرك المخاطر الأمنية المرتبطة بنماذج الذكاء الاصطناعي، مثل احتمالية تزيف البيانات أو اختراق الخوارزميات (Model Poisoning) لتضليل النتائج.	6
المحور الثاني: مصادر الوعي بالأمن السيبراني.				
			يساهم التكوين الجامعي في تعزيز وعيي بأسس الأمن السيبراني	7
			تساهم المواقع التقنية والمنصات العلمية المتخصصة في زيادة إدراكي للمخاطر السيبرانية المعاصرة	8
			أستفيد من المنصات التقنية والمجتمعات البرمجية في متابعة قضايا الأمن السيبراني.	9
			تغطي المحاضرات والدروس الجامعية الجوانب التقنية والبرمجية للأمن السيبراني بشكل كافٍ.	10
			تساهم المصادر الأكاديمية والمراجع العلمية في تطوير معرفتي بالأمن السيبراني.	11
			أكتسب مهارات حماية الأنظمة والبيانات من خلال التطبيق العملي في المخابر الجامعية والتدريبات التقنية المتخصصة.	12
المحور الثالث: الممارسات والسلوكيات الرقمية للطلبة				
			أستخدم تقنيات المصادقة الثنائية وإدارة كلمات المرور المعقدة لتأمين الوصول الى حساباتي.	13
			أجتنب مشاركة بيانات الاعتماد (Credentials) أو الأكواد البرمجية الخاصة عبر المنصات غير المشفرة.	14

			15	أقوم بفحص عناوين الروابط (URLs) بدقة للتأكد من خلوها من محاولات التصيد الاحتيالي قبل التفاعل معها.
			16	أستخدم برامج الحماية وتحديث الأنظمة بشكل دوري.
			17	ألتزم بتطبيق مبادئ 'الأمن منذ التصميم' (Security by Design) عند بناء النظم البرمجية، مع التركيز على تأمين واجهات البرمجة (APIs) ومنع تسريب البيا
			18	أتحقق من صلاحيات الوصول Permissions التي تطالبها التطبيقات قبل تثبيتها على جهازي لضمان خصوصية البيانات
			19	أتنجذب تبادل بيانات غير مشفرة أو الدخول إلى أنظمة حساسة عزد الاتصال بشبكات Wi-Fi العامة.
المحور الرابع: إدراك التهديدات السيبرانية وانعكاساتها				
			20	أدرك أن الأنظمة التقنية للمؤسسات هي الهدف الرئيسي للهجمات السيبرانية الكبرى.
			21	أدرك أن خطر الاختراق يهدد سلامة قواعد البيانات الضخمة وأمن المعلومات الحساسة
			22	أدرك أن الهجمات السيبرانية تؤدي إلى تعطل الخدمات التقنية وفقدان سلامة البيانات في المؤسسات.

الملاحق

			أدرك أن سوء إدارة الوصول إلى الأنظمة والمنصات يفتح ثغرات أمنية للاختراق والتجسس.	23
			أدرك بأن نقص الوعي التقني هو الثغرة الأساسية التي تسهل نجاح الهجمات السيبرانية.	24
			أدرك أن الأخبار الزائفة هي وسيلة لتهديد أمن المعلومات وتضليل المستخدمين.	25
المحور الخامس: تقييم دور الجامعة وسبل التعزيز				
			تفعيل دور الجامعة في نشر ثقافة الأمن السيبراني من خلال برامج توعوية مستمرة.	26
			إدراج مقياس الأمن السيبراني كمادة أساسية ضمن المسار الدراسي لمختلف التخصصات.	27
			تنظيم ندوات وملتقيات تقنية دورية لمناقشة طرق الحماية من التهديدات السيبرانية.	28
			توفير ورشات عمل تطبيقية ومخابر متخصصة لتدريب الطلبة على التصدي للاختراقات.	29
			تعزيز الشراكة بين الجامعة والمؤسسات التقنية لتطوير المهارات الأمنية لدى الطلبة.	30
			تكثيف الحملات الرقمية التوعوية حول الاستخدام الآمن للأنظمة والبيانات الجامعية.	31