الجمهورية العربية السورية
وزارة التعليم العالي والبحث العلمي
الجامعة الافتراضية السورية
ماجستير إدارة التقانة

مدى الوعي الأمني بالمخاطر والتهديدات السيبرانية- دراسة استكشافية بين طلبة الجامعات في سورية

The level of security awareness of cyber risks and threats - an exploratory study among university students in Syria

بحث مقدم لنيل درجة الماجستير في إدارة التقانة PMTM

إعداد الطالب

مازن سهيل تلجه

Mazen_256803

إشراف:

د. لؤي صالح

2024

الملخص

هدف هذا البحث إلى الإضاءة على مفاهيم الأمن السيبراني، واستكشاف مدى الوعي بين طلاب الجامعات لمخاطر الأمن السيبراني. تم جمع البيانات من خلال استبيان تم توزيعه على عينة من طلبة الجامعات في مختلف التخصصات.

أظهرت النتائج أن الطلبة يستشعرون أهمية بالغة لمفاهيم الأمن السيبراني لكن وعيهم الحقيقي للمخاطر السيبرانية متوسط عموماً، فهم لم يتلقوا أي تدريب في هذا المجال، وقد جاءت معرفتهم بتهديدات الأمن السيبراني غالبًا من تجاربهم الشخصية ومن مصادر معلومات عامة كوسائل التواصل الاجتماعي والمقالات الإلكترونية. كما أبدى الطلبة جهلاً واضحاً بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في الجمهورية العربية السورية (قد يكون هذا الجهل مبرراً نظراً لحداثة هذه القوانين).

فيما يتعلق بالتعرف على التهديدات، أدرك الغالبية من المشاركين وجود نوع محدد من التهديدات وهو الفيروسات، لكن المخاطر الأخرى كالتصيد الاحتيالي وهجمات Ddos وغيرها كانت أقل شهرة. كما أكدت النتائج أن نسبة من الطلبة لا تستخدم كلمات مرور قوية أو برامج حماية مخصصة. بالإضافة إلى ذلك، شعرت الغالبية العظمى من العينة بعدم ثقة في قدرتها على التعامل مع الهجمات السيبرانية، مما يستدعي تعزيز المهارات العملية والتدريب في هذا المجال.

أوصت الدراسة بضرورة تعزيز البرامج التعليمية والتدريبية في مجال الأمن السيبراني داخل الجامعات وذلك بهدف رفع مستوى الوعي والمهارات لدى الطلبة لمواجهة التهديدات المتزايدة.

الكلمات المفتاحية: أمن المعلومات- الأمن السيبراني- حماية البيانات.

Abstract

This research aimed to shed light on the concepts of cybersecurity and explore the awareness of university students of cybersecurity risks. Data were collected through a questionnaire distributed to a sample of university students in various disciplines

The results showed that students feel the great importance of cybersecurity concepts, but their real awareness of cyber risks is generally average, as they have not received any training in this field, and their knowledge of cybersecurity threats often came from their personal experiences and from general information sources such as social media and electronic articles. Students also showed clear ignorance of the legislation and laws related to cybercrimes in the Syrian Arab Republic (this ignorance may be justified given the recentness of these laws)

In terms of recognizing threats, the majority of participants realized the existence of a specific type of threat, which is viruses, but other risks such as phishing and DDoS attacks and others were less well-known. The results also confirmed that a percentage of students do not use strong passwords or dedicated protection programs. In addition, the vast majority of the sample felt a lack of confidence in their ability to deal with cyber attacks, which calls for enhancing practical skills and training in this field. The study recommended the need to enhance educational and training programs in the field of cyber security within universities in order to raise the level of awareness and skills among students to confront the increasing threats.

فهرس المحتويات

الفصل الأول

الإطار العام للدراسة

1-1- مقدمة:

في عصر المعلومات الرقمية المتسارع، أصبحت نظم المعلومات جزءًا لا يتجزأ من العمليات اليومية للمؤسسات والأفراد. تتيح هذه النظم تخزين البيانات، ومعالجتها، وتبادلها، مما يسهم في تحسين الكفاءة وتعزيز اتخاذ القرارات. ومع ذلك، فإن تزايد الاعتماد على التكنولوجيا الرقمية قد أدى أيضًا إلى ارتفاع كبير في التهديدات السيبرانية التي تستهدف هذه النظم. تشمل التهديدات السيبرانية مجموعة واسعة من الهجمات، مثل البرمجيات الخبيثة، وهجمات حجب الخدمة، والاختراقات الأمنية التي تؤدي إلى فقدان البيانات أو تسريب المعلومات الحساسة. تتطلب هذه التهديدات استراتيجيات أمان متقدمة لمواجهة المخاطر المتزايدة وضمان سلامة المعلومات.

نهدف من خلال هذا البحث إلى تقديم رؤى شاملة حول أهمية الأمن السيبراني والاستراتيجيات الفعالة لحماية نظم المعلومات، مما يسهم في تحقيق الأمان والموثوقية في عالم رقمي متزايد التعقيد.

2-1- المصطلحات والتعاريف:

- نظم المعلومات: مجموعة من الأجهزة والبرامج والبيانات والإجراءات التي تعمل معًا لجمع المعلومات ومعالجتها وتخزينها.
- الأمن السيبراني: مجموعة من الإجراءات والتقنيات المصممة لحماية نظم المعلومات من الهجمات السيبرانية، وضمان سلامة البيانات وخصوصيتها.
- التهديد السيبراني: أي حدث أو فعل يمكن أن يؤدي إلى ضرر أو فقدان بيانات أو اختراق للأنظمة. يشمل ذلك البرمجيات الخبيثة، والاختراقات، وهجمات حجب الخدمة.
- البرمجيات الخبيثة (Malware): برامج مصممة للإضرار بالأنظمة أو سرقة المعلومات. تشمل الفيروسات، الديدان، وبرامج الفدية (Ransom ware).

- اختراق البيانات: الوصول غير المصرح به إلى البيانات الحساسة، مما يؤدي إلى تسريب أو فقدان المعلومات.
- التشفير: عملية تحويل البيانات إلى صيغة غير قابلة للقراءة إلا للأشخاص المخولين، مما يحمي المعلومات من الوصول غير المصرح به.
- الجدران النارية (Firewalls): أنظمة أمان تُستخدم للتحكم في حركة البيانات الواردة والصادرة بين الشبكات، مما يحمي الشبكة من التهديدات الخارجية.

1-3- مشكلة البحث:

تتزايد التهديدات السيبرانية بشكل مستمر، مما يشكل تحديًا كبيرًا للأمن السيبراني على مستوى المؤسسات والأفراد. مع تطور التكنولوجيا وازدياد الاعتماد على نظم المعلومات، أصبحت الهجمات السيبرانية أكثر تعقيدًا وتنوعًا، مما يتطلب استراتيجيات أمان فعّالة للتصدي لهذه التهديدات.

تنبع مشكلة البحث من الأسئلة التالية:

1) ما هي أشكال التهديدات السيبرانية الحديثة وكيف تتطور؟ وكيف تؤثر على الأعمال؟
2) ما هي أوجه قصور استراتيجيات الأمان الحالية؟
3) ما هي الاستراتيجية الوطنية في سورية لتعزيز الأمن السيبراني؟
4) هل يتوافر الوعي الكافي بأخطار الأمن السيبراني لدى الأفراد في المجتمع السوري (حالة طلاب الجامعات كعينة)؟

تستدعي هذه المشاكل البحث عن حلول مبتكرة واستراتيجيات فعالة لتعزيز الأمن السيبراني، مما سيساهم في حماية نظم المعلومات وضمان استمرارية الأعمال في مواجهة التهديدات المتزايدة.

1-4- هدف البحث

يهدف هذا البحث إلى:

1) تحليل التهديدات السيبرانية الحديثة: وذلك من خلال دراسة الأنماط والتوجهات في التهديدات السيبرانية وتأثيرها على نظم المعلومات، لفهم طبيعتها وتعقيدها.
2) تقييم فعالية استراتيجيات الأمن السيبراني: وذلك من خلال تحليل الاستراتيجيات الحالية المعتمدة في المؤسسات لحماية نظم المعلومات، وتحديد نقاط القوة والضعف فيها.
3) اقتراح أفضل الاستراتيجيات لتعزيز الأمن السيبراني: وذلك من خلالاقتراح حلول لمواجهة التهديدات السيبرانية وزيادة الوعي والتدريب من خلال التركيز على أهمية توعية الموظفين وتقديم برامج تدريبية لتعزيز الثقافة الأمنية داخل المؤسسات.
4) تقييم الوعي الأمني للمخاطر السيبرانية: من خلال استبيان بين طلبة الجامعات.

1-5- أهمية البحث

1) زيادة الوعي الأمني: يسهم البحث في رفع الوعي حول التهديدات السيبرانية وآثارها المحتملة على المؤسسات، مما يعزز من ثقافة الأمان بين الموظفين والمديرين.
2) تحسين استراتيجيات الأمن السيبراني: يوفر البحث تقييمًا شاملًا للاستراتيجيات الحالية، مما يساعد المؤسسات في تحديد نقاط الضعف وتحسين ممارسات الأمان.
3) دعم الأبحاث الأكاديمية: يساهم البحث في إثراء الأدبيات الأكاديمية المتعلقة بالأمن السيبراني، مما يشجع على المزيد من الدراسات والأبحاث المستقبلية في هذا المجال.

1-6- فرضيات البحث

يستند البحث إلى الفرضيات التالية:

- الفرضية الأولى: هناك علاقة إيجابية بين مستوى التعليم وزيادة الوعي الأمني السيبراني بين الطلبة.

- الفرضية الثانية: الطلبة الذين يدرسون في تخصصات تقنية لديهم وعي أكبر بالتهديدات السيبرانية مقارنةً بتخصصات أخرى.
- الفرضية الثالثة: يزيد الاستخدام المتزايد لوسائل التواصل الاجتماعي من تعرض الطلبة للتهديدات السيبرانية.

1-7- متغيرات البحث

المتغيرات المستقلة

1. العمر
2. الشهادة
3. التخصص الأكاديمي :تقني أو غير تقني.
4. التدريب المسبق والتوعية بمفاهيم الأمن السيبراني

المتغيرات التابعة

- مستوى الوعي الأمني السيبراني.

1-8- منهجية البحث

1) يعتمد البحث على المنهج الوصفي التحليلي في وصف الظاهرة موضع الدراسة وتحليليها.

2) جمع البيانات عبر الاستبيانات وتوزيعها عبر البريد الإلكتروني أو المنصات الإلكترونية (مثل Google Forms) و تطبيق تلغرام.

3) تحليل البيانات: ويتضمن التحليل الكمي باستخدام Microsoft Excel.

4) إعداد النتائج والتوصيات.

1-9- حدود البحث

- الحدود الزمانية: الفصل الدراسي S24 في العام 2024م.
- الحدود المكانية: سورية
- الحدود البشرية: طلاب الجامعات السورية

1-10-الدراسات المرجعية

1. استراتيجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتيجي لمواجهة الإرهاب الإلكتروني في جامعة الأميرة نورة بنت عبدالرحمن. د. فاطمة بنت محمد بن سابق القحطاني 2022.

هدف البحث الى تقديم تصور مقترح لتطبيق استراتيجيات نظام الأمن السيبراني بالتخطيط الاستراتيجي لمواجهة الإرهاب الالكتروني في جامعة الأميرة نورة بنت عبد الرحمن في إدارة الأمن السيبراني، ومعرفة أسباب الإرهاب الإلكتروني، وأبرز استراتيجيات الأمن السيبراني في الجامعات، وتحديد متطلّبات تطبيق نظام الأمن السيبراني في الجامعات.استخدم البحث المنهج الوصفي بأسلوبه الوثائقي. وتوصَّلتْ النتائج إلى أهمية تطبيق استراتيجيات نظام الأمن السيبراني في الجامعات؛ وذلك من خلال توجيه القيادات الجامعية إلى التخطيط الاستراتيجيلتوفير بيئة إلكترونية آمنة، ولتطبيق أساليب حماية أنظمة تقنية المعلومات الحديثة، ولدعم الإجراءات الاحترازية، ولتصميم بروتوكولات التحقُّق وأنظمة تشفير البيانات، ولنشر التوعية بمخاطر الإرهاب الإلكتروني والتهديدات السيبرانية في الجامعات.

أوصى البحث بأهمية تنسيق وتكامل الجامعات مع الهيئة الوطنية للأمن السيبراني لإعداد برامج تعليمية وتدريبية تنمّي المهارات وتنشر الوعي لدى أفراد المجتمع السعودي للوصول إلى فضاء سيبراني سعودي آمِـــن.

2. **مدى توافر الوعي بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية.القحطانى، نورة بنت ناصر**–الإمارات العربية المتحدة 2019

هدفت هذه الدراسة إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم؛ من خلال التعرف على آرائهم حول المفهوم الأقرب له وأهم الجرائم التي يتعامل معها وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني والمعوقات المجتمعية لتحقيق الوقاية من هذه الجرائم، وقد استخدمت الدراسة منهج المسح الاجتماعي بأسلوب العينة، واعتمدت الدراسة على الاستمارة الإلكترونية لتجميع البيانات، وجاءت النتائج بأن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو "استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها"، في حين جاءت جريمة "الاحتيال الإلكتروني/النصب الإلكتروني" كأكثر جريمة يتعامل معها الأمن السيبراني؛ في حين تعتبر التوعية الإعلامية للمجتمع حول طرقه هي أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني. كما جاءت النتائج بوجود معوقات اجتماعية له في تحقيق الوقاية للمجتمع السعودي، وأن أهم هذه المعوقات هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة دون المعرفة الكاملة لمشكلات هذه الوسائل وكيفية تجنبها، وجاءت الدراسة بمجموعة من التوصيات أهمها (التوعية، وتنمية البنية التحتية للأمن السيبراني داخل المملكة، وتشديد العقوبات على جرائم الفضاء السيبراني، ونشر مناهج تعليمية داخل المراحل الدراسية المختلفة تعرف به ودور الفرد فيه، بالإضافة إلى الرقابة الأسرية للأولاد أثناء التعامل مع الإنترنت ووسائل التكنولوجيا الحديثة).

3. طواهير عبد الجليل، "استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي "، مجلة الرسالة للدراسات الإعلامية، 2023.

سعت الدراسة إلى التعرف على استراتيجيات الأمن السيبراني في ظل التهديدات التي يمثلها انعدام الأمن الإلكتروني. كما أكدت على أهمية الأمن السيبراني كجزء من الأمن القومي، مشيرة إلى تجربة دولة الإمارات العربية المتحدة في تطوير استراتيجيات فعالة لضمان تحول رقمي

آمن. توصلت الدراسة إلى أن نجاح التجربة جاء نتيجة تبني خطوات استراتيجية مدعومة بمعايير قانونية متطورة لمكافحة الجريمة الإلكترونية.

4. د. بن عديد سامية،مخاطر الامن السيبراني والمعلوماتي وتطور المعرفة التقنية على برامج الحماية للأنظمة المعلوماتية، 2023.

استهدفت الدراسة ضبط مفاهيم كلا الامن المعلوماتي والأمن السيبراني والمعرفة التقنية، وما ينجم عنها من مخاطر تستهدف بالدرجة الاولى برامج الحماية الموكل لها الحفاظ على النظام المعلوماتي، وتحديد مدى مسؤولية مالك النظام عن وضع استراتيجية أمنية محترفة.استنتجت الدراسة ان هناك عدة مستويات من الأمن، فعلى مستوى بسيط نجد أمن المعلومات والذي يتضمن حماية المعلومات والكيان المادي والمنطقي للنظام المعلوماتي سواء كان متصلا بالشبكة او خارجها، إلا انه اقل فعالية مقارنة بالأمن السيبراني الذي يبنى على اسس وقواعد اكثر حزماً ويتضمن الوقاية الاستباقية ثم الهجوم أو الردع لضمان أمن أعلى وأكثر فعالية .

أوصت الدراسة بوضع استراتجية وطنية فعالة مبنية على عدة محاور تقنية فنية من جهة وقانونية من جهة ثانية واقتصادية من جهة ثالثة والاهم تربوية توعوية.

الدراسات الأجنبية :

1- Wenye, Wang &ZhuoLu(2013). Cyber security in the Smart Grid: Survey and challenges

قامت هذه الدراسة بعمل استبيان شامل لقضايا الأمن السيبراني للشبكة الذكية، وعلى وجه التحديد ركزت على مراجعة ومناقشة متطلبات الأمان ونقاط الضعف في الشبكة والتدابير المضادة للهجوم وبروتوكولات الاتصال الآمنة في الشبكة الذكية.كما هدفت الدراسة الى توفير فهم عميق لنقاط الضعف الأمنية والحلول في الشبكة الذكية والقاء الضوء على اتجاهات البحث المستقبلية للشبكة الذكية.

2- Syed Adnan Jawaid , Cyber Security Threats to Educational Institutes: A GrowingConcern for the New Era of Cybersecurity, University of Maryland 05 November 2022

قامت هذه الدراسة بالتركيز على أنشطة التعليم عن بعد وخاصة المؤتمرات الفيديوية والحوسبة السحابية وخاصة بعد انتشار فيروس كوفيد-19 حيث أصبح استخدامها بشكل أكبر بكثير في التعليم مما كان عليه سابقاًنظراللإجراءاتالوقائية،وأوضحتالإختراقات السيبرانية من خلال سرقة البريد الإلكتروني ونقل البيانات والتحكم في الأجهزة التي يستخدمها المشاركون في المؤتمر وأوصت باتخاذ سياسات أمنية التي تقيد الوصول إلى الموارد والتطبيقات وتحديث تصحيحات الأمان واستخدام بروتوكولات التشفير.

3- Harnessing the capabilities of artificial intelligence to improve cybersecurity, Zeadally 2020

أوضحت الدراسة وهي بعنوان " تسخير قدرات الذكاء الاصطناعي لتحسين الأمن السيبراني" أنّ على مدى السنوات العشر الماضية، أصبح الأمن السيبراني مجالًا سريع التطور وظهر في الأخبار بشكل متكرر بسبب زيادة التهديدات والجهود المستمرة التي يبذلها المتسللون للتغلب على تطبيق القانون. بمرور الوقت، قام مجرمو الإنترنت بتحسين أساليبهم، على الرغم من أن دوافعهم الأولية للقيام بالهجمات الإلكترونية ظلت ثابتة إلى حد ما. إن قدرة أنظمة الأمن السيبراني التقليدية على تحديد وإيقاف عمليات الاختراق الجديدة آخذة في التضاؤل. إن التطورات التكنولوجية في مجال التشفير والذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق، لديها القدرة على تمكين المتخصصين في مجال الأمن السيبراني من مكافحة التهديدات الديناميكية التي يقدمها الخصوم. هنا، ندرس كيف يمكن للذكاء الاصطناعي أن يعزز حلول الأمن السيبراني من خلال الإشارة إلى مزاياه وعيوبه. نتحدث أيضًا عن الاتجاهات المحتملة للدراسة المستقبلية حيث يتم تطوير مناهج الذكاء الاصطناعي في الأمن السيبراني عبر مجموعة متنوعة من قطاعات التطبيقات.

التعقيب على الدراسات السابقة (الفجوة البحثية)

- غالبية الدراسات تركز على طلبة الجامعات بشكل عام دون النظر إلى الفروق بين التخصصات الأكاديمية، مما قد يؤدي إلى نتائج غير دقيقة.
- قلة الدراسات التي تبحث في تأثير البرامج التعليمية المتخصصة في الأمن السيبراني على سلوكيات الطلبة، مما يشير إلى حاجة ملحة لدراسات تقيّم فعالية هذه البرامج.
- هناك فجوة بين معرفة الطلبة بالمخاطر السيبرانية وسلوكياتهم الفعلية في الحماية. معظم الدراسات تركز على المعرفة النظرية دون تحليل كيفية تطبيق هذه المعرفة في الحياة اليومية.

1-11- خطة البحث:

1) الفصل النظري ويتضمن:

- مقدمة تتضمن تقديم خلفية حول أهمية أمان نظم المعلومات. وتوضيح مشكلة البحث وأهدافه وعرض فرضيات البحث.
- مراجعة الأدبيات واستعراض الدراسات السابقة المتعلقة بالأمن السيبراني والتهديدات السيبرانية.

2) الفصل العملي ويتضمن:

- جمع البيانات وإجراء الاستبيانات.
- تحليل البيانات
- تقديم النتائج المستخلصة ومناقشتها وتفسيرها.

3) خاتمة البحث.

الفصل الثاني

الإطار النظري للدراسة

2-1- مفهوم الأمن السيبراني

مصطلح السيبرانية هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي. كلمة "Cyber" هي لفظ يوناني الأصل مشتق من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للتعبير عن المتحكم.[ويرجع العديد من المؤرخين أصلها إلى عالم الرياضيات الأمريكي Norbert Wieners وذلك للتعبير عن التحكم الآلي فهو الأب الروحي المؤسس للسبرنيتيقية، وأشار في كتابه إلى أن السبرنتيقيةهي التحكم والتواصل عند الحيوان والآلة والإنسان ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب..[2]ويرى البعض أن السيبرانية كلمة انجليزية مشتقة من كلمة "Cyber" وتعنى مرتبط بالحاسب الآلي أو شبكات الحاسب، وتعني أيضاً فضاء الانترنت أو العالم الافتراضي.

نورد فيما يلي مجموعة المفاهيم المرتبطة بكلمة "سيبراني":

- **مفهوم الفضاء السيبراني:** مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الإنترنت وكم هائل من البيانات والمعلومات والأجهزة, كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة[3].كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) على أنه "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري والذي يعد جزءاً أساسياً في فهم الفضاء السيبراني.كما عرفه الاتحاد الدولي للاتصالات بأنه "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم ومستخدمي كل هذه العناصر[3].وعليه يمكننا القول بأن: " الفضاء السيبراني هو بيئة تفاعلية حديثة تشمل عناصر مادية وغير مادية مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين أو مستعملين."

- **مفهوم المخاطر السيبرانية:** أي المخاطر التي تتعلق بالخسارة المالية أو الاضطراب أو الإضرار بسمعة منظمة بسبب شكل من أشكال فشل نظام تكنولوجيا المعلومات الخاص بها، وتشمل مكونات المخاطر السيبرانية التهديدات الحالية ونقاط الضعف والقيم المعرضة للخطر (الأصول والسمعة).
- **مفهوم الأمن السيبراني:** يعرف 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 على الأقل الحد من آثارها.[1]يعرف فريتشاردكمرر[6] الأمن السيبراني بأنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة."بينما عرفه إدوارد أمورسو[2]على أنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها.
- **مفهوم القوة السيبرانية:** هي مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات، المعلومات، الشبكات الإلكترونية، البنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل.كما تعرف القوة السيبرانية بأنها القدرة على القيام بنشاط سيبراني مؤثر في الفضاء السيبراني أو القدرة على استخدام الفضاء السيبراني لتحقيق مجموعة من الأهداف والتأثير على الأحداث, وتعرف أيضاً على أنها الموارد البشرية والمادية المتاحة ضمن بيئة استراتيجية يمكن استخدامها لإحداث تأثير في الفضاء السيبراني[5].
- **مفهوم الاستراتيجية السيبرانية:** هي تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني متكاملة مع المجالات العملياتية الأخرى لتحقيق أو دعم تحقيق الأهداف عبر عناصر القوة الوطنية، وتعتمد الاستراتيجية السيبرانية على مزيج منظم من الغايات والوسائل والطرق لتحقيق أهداف الأمن العسكري والسياسي والاقتصادي والمعلوماتي والوطني الأوسع من خلال الاعتماد على القدرات السيبرانية وتوفير الموارد والتكاليف الواجب اتخاذها لمواجهة المخاطر خاصة السيبرانية[24].

- **مفهوم الإرهاب السيبراني (الإلكتروني) :** ينطلق تعريفه من تعريف الإرهاب حيث لا يختلف كلاهما إلا في نوعية الأداة أو الوسيلة المستخدمة لتحقيق العمل الإرهابي، وكانت بداية استخدام مصطلح الإرهاب الإلكتروني في فترة الثمانينات علي يد "باري كولين"[4]،الذي عرف الإرهاب الإلكتروني بأنه: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب.ويعرفه جيمس لويس[4]: بأنه استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنية التحتية الوطنية المهمة مثل الطاقة والنقل والعمليات الحكومية أو بهدف ترهيب حكومة ما أو مدنيين.أما دورثيدينينغ وهي من أبرز الباحثين في مجال الأمن الإلكتروني ترى أن الإرهاب الإلكتروني: هو الهجوم القائم على مهاجمة الحاسوب وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب.[4]
- **مفهوم الهجمات السيبرانية:** تعرف بأنها مجموعة من الأنشطة الإلكترونية التي تتخذ من طرف سواء أكان تابعاً لدولة أم يعمل لحسابها بصورة مستقلة عنها في دولة ما ضد نظم إلكترونية تابعة لدولة أخرى يراد منها التغلغل إلى تلك النظم بهدف السيطرة على قوتها الإلكترونية ومن ثم التحكم بها عن بعد لأجل إحداث أكبر قدر ممكن من الأضرار.ووفقاً لمبادئ (تالين) بشأن الحروب السيبرانية [5]عرفت الهجمات السيبرانية بأنها "عمليات سيبرانية سواء أكانت هجومية أم دفاعية والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأهداف."كما عرفها مايكل شميت[5]: بأنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.
- **مفهوم الجريمة السيبرانية:** تعرف الجريمة السيبرانية بالمعنى الضيق على أنها "جريمة الكمبيوتر"، وأي تصرف غير قانوني موجه ضد الجهاز والنظام أو المعلومات التي تحويه، أما بمعناها الواسع فهي الجريمة المتصلة باستخدام الكمبيوتر وأي تصرف غير قانوني يرتكب باستخدام تقنيات المعلومات والاتصالات بما فيه حيازة مواد ممنوعة أو توزيعها أو عرضها.كما تعرف بأنها مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو

أجهزة إلكترونية أو شبكة الانترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها[1].

2-2- أنواع التهديدات والهجمات السيبرانية الشائعة

نورد فيما يلي أهم أنواع الهجمات السيبرانية:

2-2-1- البرمجيات الخبيثة (Malware):

هي مصطلح يشمل جميع الأنواع من البرامج الضارة التي تهدف إلى إلحاق الضرر بالأنظمة أو الشبكات أو البيانات. وهي أبرز التهديدات السيبرانية التي تواجه الأفراد والمؤسسات. وتعتبر تهديدًا خطيرًا يتطلب استجابة سريعة وفعالة, من خلال اتخاذ الاحتياطات اللازمة، يمكن للأفراد والمؤسسات تقليل مخاطر الإصابة بهذه الأنواع من البرامج.

من أنواع البرمجيات الخبيثة[7]:

- الفيروسات (Viruses):وهي برامج ضارة تتصل بملفات أخرى وتقوم بتكرار نفسها عند فتح الملف المصاب.بحيث يمكن أن تتسبب في إتلاف البيانات أو تعطل النظام.
- الديدان (Worms): وهي نوع من البرمجيات الخبيثة التي تنتشر عبر الشبكات دون الحاجة إلى تدخل المستخدم.ويمكن أن تؤدي إلى استهلاك موارد الشبكة وتسبب بطء في الأداء.
- البرمجيات الفدية (Ransomware): تقوم بتشفير بيانات المستخدمين وتطلب فدية لإعادتها.وتؤدي إلى فقدان الوصول إلى البيانات الهامة وقد تتسبب في خسائر مالية كبيرة.
- تروجان (Trojan Horses): وهي برامج تبدو شرعية ولكنها تحتوي على أكواد ضارة، تقوم بفتح ثغرات في النظام، حيث تؤدي إلى سرقة البيانات أو تثبيت برمجيات خبيثة أخرى.
- البرمجيات التجسسية (Spyware):تهدف إلى جمع المعلومات عن المستخدمين دون علمهم، مثل كلمات المرور وبيانات بطاقة الائتمان.مما يؤدي إلى انتهاك الخصوصية وتعرض المعلومات الحساسة للخطر.

- البرمجيات الإعلانات (Adware:تعرض إعلانات غير مرغوب فيها وتجمع معلومات عن سلوك المستخدم، وقد تؤدي إلى بطء في النظام وتجربة مستخدم مزعجة.

يمكن الحماية من البرمجيات باتباع الاستراتيجيات التالية:

- استخدام برامج مكافحة الفيروسات وتحديثها بشكل دوري.
- تحديث النظام والتطبيقات :التأكد من تحديث جميع الأنظمة والبرمجيات بانتظام لسد الثغرات الأمنية.
- تجنب الروابط غير المعروفة :الحذر عند فتح الروابط أو المرفقات في الرسائل الإلكترونية.
- استخدام جدران الحماية :تفعيل جدران الحماية لحماية الشبكة من الهجمات الخارجية.
- التوعية والتدريب :زيادة وعي المستخدمين بالمخاطر المحتملة وكيفية التعامل معها.

2-2-2- التصيد الاحتيالي (Phishing):

هو نوع من الهجمات السيبرانية التي تهدف إلى خداع الأفراد للحصول على معلومات حساسة، مثل كلمات المرور، وأرقام بطاقات الائتمان، والبيانات الشخصية، من خلال انتحال هوية جهة موثوقة. يحدث التصدي الاحتيالي عبر الوسائل التالية [8]:

- رسائل البريد الإلكتروني المزيفة: يقوم المهاجم بإرسال رسائل بريد إلكتروني تبدو وكأنها من مصادر موثوقة (مثل البنوك أو الشركات الكبرى) تشمل روابط أو مرفقات ضارة.
- مواقع الويب المزيفة: يُطلب من الضحية زيارة موقع ويب يبدو شرعيًا، حيث يتم حثه على إدخال معلوماته الحساسة.
- الرسائل النصية : يستخدم المهاجمون الرسائل النصية لإرسال روابط أو طلبات معلومات، مشابهة لهجمات التصيد عبر البريد الإلكتروني.
- المكالمات الهاتفية: انتحال هوية جهات موثوقة عبر الهاتف للحصول على معلومات حساسة.

من أنواع التصيد الاحتيالي:

- التصيد التقليدي: يتم من خلال رسائل البريد الإلكتروني والمواقع المزيفة.

- التصيد المستهدف (Spear Phishing): يستهدف أفرادًا أو مجموعات معينة بناءً على معلومات مسبقة عنهم، مما يجعله أكثر خطورة.
- التصيد عبر وسائل التواصل الاجتماعي: استخدام المنصات الاجتماعية لخداع المستخدمين للحصول على معلوماتهم أو توجيههم لمواقع ضارة.
- التصيد عبر التطبيقات:يمكن أن يحدث من خلال تطبيقات الهواتف الذكية التي تبدو شرعية.

يمكن الحماية من التصيد الاحتيالي عبر الوسائل التالية:

- التأكد من المرسل: تحقق من عنوان البريد الإلكتروني وتأكد من أنه يتطابق معالمصدر المعروف.
- عدم النقر على الروابط: تجنب النقر على الروابط المشبوهة أوالمرفقات في الرسائل غير المعروفة.
- استخدام أدوات الحماية: تثبيت برامج مكافحة الفيروسات واستخدام أدوات الحماية من التصيد.
- التوعية والتدريب: تعزيز الوعي حول أساليب التصيد الاحتيالي وكيفية التعرف عليها.
- تفعيل المصادقة الثنائية: استخدام المصادقة الثنائية عند توفرها لحماية الحسابات.

2-2-3- الاختراق Hacking

الاختراق هو عملية استغلال نقاط الضعف في أنظمة الحواسيب أو الشبكات للوصول غير المصرح به إلى المعلومات أو التحكم في الأنظمة. يمكن تصنيف الاختراق إلى [9]:

- الاختراق الضار(Malicious Hacking): يشير إلى الأنشطة غير القانونية التي يقوم بها المهاجمون للوصول إلى الأنظمة أو البيانات بغرض السرقة أو التخريب.ويؤدي إلى فقدان البيانات، سرقة المعلومات، أو تعطيل الخدمات.

- الاختراق عبر الشبكات(Network Hacking): استغلال الثغرات في الشبكات للوصول إلى المعلومات أو الأنظمة، بحيث يمكن أن يؤدي إلى انقطاع الخدمات أو سرقة البيانات.
- اختراق التطبيقات(Application Hacking):استغلال الثغرات في البرمجيات أو التطبيقات،يمكن أن يؤدي إلى تسريب البيانات أو السيطرة على التطبيقات.

يحدث الاختراق وفق التقنيات التالية:

- استغلال الثغرات (Exploiting Vulnerabilities):أي استخدام نقاط الضعف المعروفة في البرمجيات أو الأنظمة.
- الهندسة الاجتماعية (Social Engineering):خداع الأفراد للحصول على معلومات حساسة.
- تحليل الشبكة (Network Sniffing):مراقبة حركة البيانات على الشبكة لاكتشاف المعلومات السرية.

يمكن الحماية من الاختراق باتباع الاستراتيجيات التالية:

- تحديث الأنظمة والتطبيقات بشكل دوري لسد الثغرات الأمنية.
- تفعيل جدران الحماية
- تطبيق بروتوكولات الأمان :اعتماد ممارسات أمان قوية، مثل استخدام كلمات مرور قوية والمصادقة الثنائية.
- التوعية والتدريب :تعليم المستخدمين حول مخاطر الاختراق وكيفية تجنبه.

2-2-4- هجوم الرجل الوسيط(Man-in-the-Middle Attack –MitM)

هو نوع من الهجمات السيبرانية حيث يتدخل المهاجم في الاتصال بين طرفين (مثل جهاز كمبيوتر وموقع ويب) دون علمهما. يهدف المهاجم إلى مراقبة أو تعديل المعلومات المتبادلة بين الطرفين.يقوم

المهاجم باعتراض البيانات المتبادلة بين الطرفين، مما يسمح له بمراقبة الرسائل والمعلومات الحساسة. كما يمكنه التلاعب بالمعلومات المرسلة أو المستلمة، مثل تغيير تفاصيل المعاملات المالية. أيضاً يمكن للمهاجم انتحال شخصية أحد الأطراف، مما يجعل الطرف الآخر يعتقد أنه يتواصل مع جهة موثوقة[10].

يتم تنفيذ هجوم الرجل الوسيط عبر الوسائل التالية:[10]

- شبكات الوايفاي العامة:يمكن للمهاجم إنشاء نقطة اتصال واي فاي مزيفة، مما يسمح له بالتنصت على البيانات التي تتبادلها الأجهزة المتصلة.
- التشويش على اتصالات الشبكة:استخدام تقنيات مثل ARP Spoofing لاستغلال نقاط الضعف في الشبكات لجعل البيانات تمر عبر جهاز المهاجم.
- البرمجيات الخبيثة:تثبيت برامج ضارة على جهاز الضحية يمكن أن تسمح بالتحكم في الاتصالات.

يمكن الحماية من هجوم الرجل الوسيط عبر استخدام بروتوكولات التشفير(مثل HTTPS و TLS) لضمان أن البيانات المتبادلة، وتجنب استخدام الشبكات العامةأو غير المأمونة، خاصة عند تبادل المعلومات الحساسة. كذلك من الضروري التأكد من صحة الهوية عند التواصل مع جهات عبر الإنترنت.

2-2-5- الهجوم الموزع لتعطيل الخدمة(DdoS) :

هو نوع من الهجمات السيبرانية التي تهدف إلى جعل خدمة أو موقع ويب غير متاح عن طريق استهدافه بكمية هائلة من حركة المرور، مما يتسبب في تعطيل عمله.يتبع هذا الهجوم الاستراتيجيات التالية:

- **تجميع الزومبيات(Botnets)** :يتم استخدام أجهزة كمبيوتر مخترقة، تُعرف بالزومبيات، لتكوين شبكة من الأجهزة التي تنفذ الهجوم بشكل متزامن.
- **إغراق الخادم أو الشبكة:**ترسل هذه الأجهزة كميات هائلة من الطلبات إلى الخادم المستهدف، مما يؤدي إلى استهلاك جميع الموارد المتاحة.

- **تعطيل الخدمة:**نتيجة الزيادة المفاجئة في الطلبات، يتعذر على الخادم معالجة الطلبات الشرعية، مما يؤدي إلى توقف الخدمة.

من أنواع هجماتDdoS:[11]

- هجمات الطبقة السابعة(Application Layer Attacks) :تستهدف التطبيقات والخدمات، مثل إرسال طلبات معقدة تؤدي إلى استهلاك الموارد.
- هجمات الطبقة الرابعة(Transport Layer Attacks) : تستهدف الشبكة والبروتوكولات، مثلTCP SYN Flood ، حيث يُرسل عدد هائل من حزم البيانات إلى الخادم.
- هجماتUDP Flood :تركز على إغراق الخادم بحزمUDP ، مما يؤدي إلى استهلاك عرض النطاق الترددي.

يؤدي هجومDDoS إلى تعطيل الخدماتوخسائر مالية، وتأثير على السمعةإذ يمكن أن يؤدي إلى فقدان الثقة من العملاء والمستخدمين.

يمكن الحماية من هجومDDoS عبر اتباع الطرق التالية:

- استخدام خدمات الحماية: الاستعانة بمزودي خدماتDdoSالذين يمكنهم تصفية حركة المرور الضارة.
- زيادة الموارد: تحسين البنية التحتية لمواجهة الزيادة المفاجئة في الطلبات.
- توزيع المحتوى: استخدام شبكات توزيع المحتوى (CDN) لتخفيف الضغط عن الخادم الرئيسي.
- تحديد حركة المرور:استخدام قواعد لتحديد حركة المرور والتحكم فيها، مثل وضع قيود على عدد الطلبات من نفس العنوان.

2-2-6- التهديد المستمر المتقدم(APT) :

هو نوع من الهجمات السيبرانية التي تستهدف المؤسسات بشكل ممنهج وطويل الأمد، حيث يسعى المهاجمون للحصول على معلومات حساسة أو سرقة بيانات دون اكتشافهم. تعتبر APTs معقدة وتتطلب تخطيطًا دقيقًا وتنسيقًا عالياً، إذ أنها تتسم بما يلي:

- الاستمرارية: تستمر هذه الهجمات لفترة طويلة، حيث يقوم المهاجمون بالعمل على تحقيق أهدافهم على مدى فترة زمنية، مما يجعل اكتشافهم أكثر صعوبة.
- الاستهداف: تركز APTs عادة على أهداف محددة مثل الحكومات، المؤسسات المالية، الشركات الكبرى، أو البنية التحتية الحيوية.
- التعقيد: يستخدم المهاجمون تقنيات متقدمة وأساليب متعددة للاختراق والبقاء مختبئين داخل الأنظمة المستهدفة.
- التخفي: يحاول المهاجمون تجنب الكشف عن وجودهم من خلال استخدام أساليب مثل التشفير وتقنيات الهندسة الاجتماعية.

يبدأ APTs من الاستطلاع، حيث جمع المعلومات حول الهدف، بما في ذلك تحديد الثغرات المحتملة. ثم تنفيذ هجوم أولي لاختراق الأنظمة، غالبًا ما يتم عبر التصيد الاحتيالي أو استغلال الثغرات. ثم ينتقل الهجوم إلى التحكم حيث يقوم المهاجمون بتثبيت أدوات التحكم للوصول المستمر. بعدها يجري التوسعفي محاولة زيادة الوصول إلى أنظمة وبيانات إضافية داخل الشبكة المستهدفة. وينتهي الهجوم بسرقة المعلومات الحساسة أو البيانات القيمةمع الحفاظ على وجودهم داخل النظام دون اكتشافهم، مما يسمح لهم بالعودة في أي وقت.

يمكن الحماية منAPTs عبر مايلي:

- الوعي والتدريب: تدريب الموظفين على التعرف على أساليب الهجمات، مثل التصيد الاحتيالي.
- تحليل السلوك: استخدام أدوات لرصد الأنشطة غير المعتادة داخل الشبكة.
- تحديث الأنظمة :التأكد من تحديث البرمجيات بصورة دورية لسد الثغرات الأمنية.
- تطبيق استراتيجيات أمان متعددة الطبقات:استخدام جدران الحماية، وبرامج مكافحة الفيروسات، وتقنيات التشفير.
- استجابة سريعة: تطوير خطط استجابة للحوادث للحد من الأضرار في حالة وقوع هجوم التهديد الداخلي من أشخاص حانقين على الشركة أو مهملين.

2-3- أنواع الأمن السيبراني

يمكن تصنيف الجوانب المعنية بالأمن السيبراني إلى:

2-3-1- أمن التجهيزات الحاسوبية:

وهو فرع من فروع الأمن السيبراني يركز على حماية الأجهزة المادية، مثل الحواسيب، والخوادم، والأجهزة المحمولة، من التهديدات والمخاطر التي قد تؤثر على سلامتها ووظيفتها. يشمل هذا النوع من الأمن مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الأجهزة من الوصول غير المصرح به، والأضرار، والسرقة. منها:[12]

- الحماية المادية: وهو تأمين الأجهزة من التهديدات الفيزيائية مثل السرقة أو الأضرار.باستخدام تقنيات مثل الأقفال، الكاميرات، أنظمة الإنذار، وأماكن التخزين الآمنة.
- أمان نظام التشغيل: وهو تأمين نظام التشغيل ضد التهديدات مثل الفيروسات والبرمجيات الضارة، وذلك بتحديث النظام بانتظام، استخدام برامج مكافحة الفيروسات، وتطبيق تصحيحات الأمان.
- التحكم في الوصول: وهو التأكد من أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى الأجهزة، عن طريق استخدام كلمات المرور، المصادقة متعددة العوامل، وأنظمة إدارة الهوية.
- التشفير: أي حماية البيانات المخزنة على الأجهزة باستخدام التشفير، عن طريق استخدام برامج تشفير القرص الكامل وتشفير الملفات الحساسة.
- النسخ الاحتياطي: إنشاء نسخ احتياطية للبيانات الهامة على الأجهزة، وذلك استخدام حلول النسخ الاحتياطي السحابية أو التخزين الخارجي.
- الرصد والمراقبة: مراقبة الأنشطة على الأجهزة لاكتشاف أي سلوك غير طبيعيباستخدام برامج رصد الشبكة وأنظمة كشف التسلل.

2-3-2- أمن البريد الإلكتروني:

هو مجموعة من الممارسات والتقنيات المصممة لحماية الاتصالات عبر البريد الإلكتروني من التهديدات والمخاطر. يعتبر البريد الإلكتروني أحد أكثر وسائل التواصل استخدامًا، مما يجعله هدفًا رئيسيًا للهجمات السيبرانية، مثل التصيد الاحتياليPhishing والبرمجيات الخبيثةMalware والرسائل غير المرغوب فيها (Spam)و هجمات انتحال الهوية (Spoofing) أي انتحال شخصية مرسل موثوق به لإرسال رسائل بريد إلكتروني مضللة.

2-3-3- أمن الشبكات:

هو مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية الشبكات من التهديدات والهجمات السيبرانية. يتضمن ذلك تأمين البنية التحتية للشبكة، وحماية البيانات المتداولة عبر الشبكات، وضمان توافر الخدمات. ومن مكونات أمن الشبكات:[3]

- جدران الحماية (Firewalls): وهي أجهزة أو برمجيات تعمل كحاجز بين الشبكة الداخلية والإنترنت، وتتحكم في حركة المرور. وظيفتها حظر الوصول غير المصرح به ومنع الهجمات.
- أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS): وهي أدوات تراقب الشبكة للكشف عن الأنشطة المشبوهة. حيث أن IDS تنبه المسؤولين عن الشبكة، بينما IPS يمكن أن تتخذ إجراءات لمنع الهجمات.
- تشفير البيانات:استخدام تقنيات تشفير لحماية البيانات أثناء النقل عبر الشبكات. وذلك لضمان سرية البيانات وحمايتها من التنصت.
- التحكم في الوصول (Access Control): وهي تقنيات لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى الشبكة. باستخدام كلمات المرور، والمصادقة الثنائية، ونظم إدارة الهوية.
- VPN (الشبكات الافتراضية الخاصة):تقنية تتيح إنشاء اتصال آمن بين المستخدمين والشبكة، وذلك بتشفير البيانات وحماية الخصوصية عند استخدام الشبكات العامة.

2-3-4- أمن البيانات والمعلومات:

وهو مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية البيانات والمعلومات من الوصول غير المصرح به، والسرقة، والتلف، والفقدان. يشمل ذلك جميع أنواع البيانات، سواء كانت رقمية أو مادية، ويعتبر جزءًا أساسيًا من استراتيجيات الأمن السيبراني. تتضمن مكونات أمن البيانات والمعلومات:[3]

- تشفير البيانات: تحويل البيانات إلى صيغة غير قابلة للقراءة إلا للأشخاص المصرح لهم، وذلكباستخدام بروتوكولات تشفير مثل AES وRSA لحماية البيانات أثناء النقل أو التخزين.
- إدارة البيانات: تنظيم البيانات وحمايتها وفقًا للسياسات والإجراءات المحددةباستخدام قواعد البيانات المدارة بشكل جيد وأنظمة إدارة المحتوى.
- تصفية البيانات: استخدام أدوات لفحص البيانات واكتشاف أي معلومات حساسة أو غير مصرح بها، مثل أدوات تحليل البيانات وأنظمة إدارة الوصول.

2-3-5- أمن التطبيقات:

هو عملية حماية البرمجيات من التهديدات السيبرانية التي تهدف إلى سرقة البيانات أو استغلال الثغرات. يشمل ذلك مجموعة من الممارسات والتقنيات لضمان سرية وسلامة وتوافر المعلومات. يتضمن أمن التطبيقات تصميم البرامج بميزات أمان قوية، وإجراء اختبارات دورية للكشف عن الثغرات، وتطبيق التحديثات الأمنية بشكل مستمر. يهدف هذا المجال إلى حماية المستخدمين والحفاظ على ثقة العملاء وسلامة البيانات.

2-3-6- أمن الحوسبة السحابية والاستضافة:

هو مجموعة من الممارسات والتقنيات المصممة لحماية البيانات والتطبيقات والخدمات التي تتم استضافتها في البيئات السحابية. يهدف هذا الأمن إلى ضمان سرية وسلامة وتوافر المعلومات، من خلال إدارة فعالة لهوية المستخدمين وصلاحيات الوصول، وتشفير البيانات لحمايتها أثناء النقل والتخزين. بالإضافة إلى ذلك، يشمل الأمن السحابي تنفيذ جدران الحماية وأنظمة كشف التسلل

لحماية البنية التحتية من الهجمات السيبرانية، مع الالتزام بالمعايير واللوائح الأمنية لضمان الامتثال القانوني. تعتبر النسخ الاحتياطية وخطط استعادة البيانات من العناصر الأساسية لضمان استمرارية العمل في حالة الطوارئ أو الكوارث.[12]

2-4- التدابير الأساسية للأمن السيبراني

يرتكز الأمن السيبراني بمفهومه الواسع على الركائز التالية:[15]

2-4-1- التدابير القانونية:

والتي تشمل مجموعة من التشريعات واللوائح المصممة لحماية البيانات وضمان الخصوصية وحماية الهوية عبر الإنترنت. تهدف هذه القوانين إلى تنظيم كيفية جمع المعلومات الشخصية واستخدامها وتخزينها ومشاركتها، مع ضمان حقوق الأفراد في الخصوصية. تتضمن أمثلة على هذه التشريعات:

- تشريعات حماية البيانات: مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تفرض قيودًا صارمة على معالجة البيانات الشخصية.
- ضمان الخصوصية: عن طريق قوانين تحمي حقوق الأفراد في الحفاظ على سرية معلوماتهم الشخصية ومنع الوصول غير المصرح به.
- حماية الهوية عبر الإنترنت: وهي إجراءات تهدف إلى منع سرقة الهوية وضمان أمان التعاملات الإلكترونية.

2-4-2- التدابير الفنية:

تشمل التدابير الفنية مجموعة من الآليات والتقنيات المصممة لحماية الأنظمة والشبكات من التهديدات السيبرانية.تسهم هذه التدابير في تعزيز الحماية السيبرانية وضمان استمرارية الأعمال من خلال تقليل المخاطر والتعامل الفعال مع الحوادث الأمنية. تتضمن هذه التدابير:

- فرق الاستجابة للحوادث السيبرانية: وهي فرق متخصصة تتولى مسؤولية الكشف عن الحوادث الأمنية والاستجابة لها بسرعة، للحد من تأثيرها واستعادة النظام إلى حالته الطبيعية.
- البرمجيات الأمنية: مثل برامج مكافحة الفيروسات وبرامج مكافحة التجسس وجدران الحماية التي تساعد في اكتشاف ومنع التهديدات السيبرانية.
- البنى الدفاعية: تشمل تصميم الشبكات بمفاهيم الأمان المدمجة، مثل الشبكات المعزولة، وأنظمة كشف التسلل (IDS)، وأنظمة منع التسلل (IPS).

2-4-3- التدابير التنظيمية

هي عبارة عن مجموعة من السياسات والإجراءات التي تهدف إلى تعزيز الأمن السيبراني على مستوى المؤسسات والدولة. تتضمن هذه التدابير:

- الاستراتيجية الوطنية للأمن السيبراني: وهي إطار شامل يحدد الأهداف والنهج اللازم لحماية البنية التحتية الرقمية للدولة. يتضمن ذلك وضع سياسات واضحة، وتحديد المسؤوليات، وتعزيز التعاون بين الجهات الحكومية والخاصة.
- التقييم الدوري: عمليات منتظمة لتقييم الوضع الأمني الحالي، تحديد نقاط الضعف، وقياس فعالية الإجراءات المطبقة. تساعد هذه التقييمات في تحسين الاستراتيجيات الأمنية وتكييفها مع التهديدات المستجدة.

2-4-4- تدابير تنمية القدرات

تشمل تدابير تنمية القدرات مجموعة من الأنشطة المصممة لتعزيز الوعي والمعرفة في مجال الأمن السيبراني. حيث تساهم في بناء قاعدة قوية من الأفراد والمؤسسات القادرة على مواجهة التهديدات السيبرانية بفعالية. وتتضمن:

- نشر ثقافة الأمن السيبراني بين العامة من خلال التعريف بالمخاطر وكيفية حماية المعلومات الشخصية.

- تنظيم فعاليات وحملات إعلامية لتثقيف المجتمع حول أهمية الأمن السيبراني وسبل الحفاظ على الأمان الرقمي.
- تقديم دورات تدريبية متخصصة للموظفين والمختصين في مجال تكنولوجيا المعلومات لتعزيز مهاراتهم في كشف التهديدات والتصدي لها.
- الحوافز الحكومية لتطوير الأمن السيبراني:وذلك بتقديم الدعم والتمويل للمبادرات والمشاريع التي تهدف إلى تعزيز الأمن السيبراني، وتشجيع الابتكار في هذا المجال.

2-4-5- التدابير التعاونية:

وهي الجهود المشتركة بين الدول والمؤسسات لتعزيز الأمن السيبراني على نطاق عالمي. هذه التدابير تساهم في تبادل المعرفة والخبرات لمواجهة التهديدات السيبرانية بفعالية. وتتضمن:

- وضع اتفاقيات دولية لتعزيز التعاون في مجال الأمن السيبراني وتبادل المعلومات حول التهديدات والهجمات.
- تنظيم مؤتمرات وندوات تجمع الخبراء والمختصين لمناقشة أحدث التطورات والتحديات في الأمن السيبراني.
- المشاركة في مبادرات وبرامج دولية تهدف إلى تعزيز القدرات الأمنية على مستوى العالم.
- بناء شراكات بين القطاعين العام والخاص لتعزيز الابتكار وتطوير حلول أمنية فعالة.

2-5- مؤشر الأمن السيبراني العالمي

مؤشر الأمن السيبراني (Global Cybersecurity Index) ويُشار له بالاختصار (GCI) هو مُبادرة من الاتحاد الدولي للاتصالات (ITU) المُنظمة الدولية الرائدة في العالم لقضايا تكنولوجيا المعلومات والاتصالات، والذي يتم من خلاله وضع معايير لحالة الأمن السيبراني للدول عبر أنحاء العالم، إذ يحتسب هذا المؤشر ويُقيّم التزام البلدان بتطبيق معايير الأمن السيبراني على المستوى العالمي. كما يمنح نظرة مُتفحصة على مُشاركة الدول ذات السيادة في الأمن السيبراني، وتجدر

الإشارة إلى أنّ هذا المؤشر العالمي هو مؤشر موثوق ومُعتمد فيما يتعلق بتقييم أداء الدول في الأمن السيبراني.

يرصد المؤشر التحسن في مستويات الوعي بأهمية الأمن السيبراني، والتدابير المتخذة لحمايته في 194 دولة من دول العالم ومن خلال 83 مؤشراً و عبر 5 أركان رئيسية، وهي التدابير القانونية، التدابير التنظيمية، التدابير التقنية، التدابير الرامية إلى تعزيز القدرات في مجال حماية الأمن السيبراني، والتدابير التي تهدف إلى تعزيز التعاون في هذا الشأن.وتحصل كل دولة على رصيد نهايته العظمى 20 درجة في كل ركن من الأركان الخمسة، ثم تُجمَع الأرصدة الخمسة لاحتساب رصيد كل دولة على المؤشر العام[16].

يقسم التقرير الصادر عن (GCI) الدول الى خمسة مستويات , ويرصد التقرير مدى التقدم الذي حققته كل دولة فيما يتعلق بالتزاماتها الفردية المتعلقة بالأمن السيبراني.يأتي المستوى الأول كأعلى المستويات الخمسة , وهو مخصص من أجل الدول التي استطاعت تقديم نموذج يحتذى به , والتي استطاعت أن تحقق التزاما قويا فيما يتعلق بجميع الركائز الخمسة الخاصة بالأمن السيبراني.أما المستوى الثاني (Advancing) فهو مخصص للدول المتقدمة في هذا المجال , والمستوى الثالث يأتي تحت عنوان التأسيس (Establishing) , أما المستوى الرابع فيحمل عنوان التطور (Evolving) , والمستوى الخامس والأخير يأتي تحت عنوان البناء (Building) .

ترتيب الدول العربية في مؤشر الأمن السيبراني العالمي 2024 :[16]

استطاعت 46 دولة أن تأتي ضمن المستوى الأول في الأمن السيبراني , ونجحت 8 دول عربية أن تكون في المقدمة , وجاء ترتيب الدول العربية في مؤشر الأمن السيبراني 2024 كالتالي :

- في المستوى الأول: كل من مصر وقطر والإمارات العربية المتحدة والمملكة العربية السعودية حيث تفوقوا في جميع الركائز.
- كما احتلت البحرين والأردن والمغرب وعمان مرتبة عالية في جميع الركائز .
- في المستوى الثالث: كل من الجزائر والكويت وليبيا وتونس .
- أما أغلب الدول العربية فجاءت في المستوى الرابع ومنهم فلسطين وسوريا والعراق ولبنان والصومال والسودان وجزر القمر . بينما جاء اليمن في المستوى الخامس .

2-6- مراجعة لأبرز الحوادث السيبرانية واستراتيجيات مواجهتها

- **وزارة التجارة الأمريكية تقترح حظر برمجيات وأجهزة السيارات من الصين وروسيا**[17]

أعلنت وزارة التجارة الأمريكية عن اقتراح حظر على استخدام برامج وأجهزة السيارات من الصين وروسيا في المركبات المتصلة على الطرق الأمريكية. يأتي ذلك بعد تحقيق حول التهديدات الأمنية الوطنية المحتملة التي تشكلها التكنولوجيا الأجنبية في المركبات. سيؤثر الحظر المقترح على جميع المركبات الصينية تقريبًا، ويحظر اختبار السيارات ذاتية القيادة من قبل خصوم أجانب، ويلزم شركات صناعة السيارات الأمريكية بإزالة بعض البرامج والأجهزة من مركباتها. إذا تمت الموافقة، فسيدخل حظر البرامج حيز التنفيذ عام 2027، وحظر الأجهزة عام 2029.

استجابة لمخاوف الأمن السيبراني الموضحة في الحظر المقترح على برامج وأجهزة السيارات الأجنبية، سيتوجب على المنظمات التركيز على ضمان فحص البرامج في المركبات المتصلة بشكل شامل وتأمينها من الثغرات المحتملة. سيساعد نشر الأدوات التي تفحص وتختبر أكواد البرامج بحثًا عن نقاط ضعف في منع الجهات الخبيثة من استغلال نقاط الضعف. بالإضافة إلى ذلك، يمكن لحلول أمان الشبكة التي تراقب وتقيد الوصول إلى الأنظمة الحرجة أن تقلل من خطر الهجمات عن بعد التي قد تعرض وظائف السيارة للخطر.

- **برنامج PEAKLIGHT الخبيث يستهدف مستخدمي Windows**

اكتشف باحثوMandiantبرنامجًا جديدًا لتوزيع البرامج الضارة يسمىPEAKLIGHT ، والذي يستهدف مستخدمي Windows من خلال تنزيلات الأفلام المزيفة. تبدأ سلسلة الهجوم المعقدة بملف اختصارWindows ، مما يؤدي إلى نشر سلالات مختلفة من البرامج الضارة بما في ذلكLumma Stealerو .Hijack Loaderتسلط هذه الحملة الضوء على المخاطر المستمرة المتمثلة في تنزيل المحتوى من مصادر غير رسمية والتكتيكات المتطورة لمجرمي الإنترنت[20] .

يجب على الشركات والمؤسسات التأكد من أن دفاعات شبكتها قادرة على فحص حركة المرور المشفرة بحثًا عن أي نشاط مشبوه دون المساس بالاستخدام المشروع، مثل الاستفادة من الأدوات التي يمكنها تحليل حركة المرور التي تمر عبر القنوات المشفرة. إن تنفيذ حلول الأمان التي يمكنها مراقبة تنفيذ نصوصPowerShell ، واكتشاف العمليات غير الطبيعية التي تعتمد على الذاكرة فقط،

ومنع تنفيذ البرامج غير المعتمدة من شأنه أن يمنع تشغيل برنامج التنزيل على النظام. يجب على المؤسسات أيضًا تعزيز أمان نقاط النهاية من خلال التحكم في الوصول إلى الأجهزة الخارجية وضمان تشغيل البرامج المصرح بها فقط على الأجهزة التي يستخدمها أعضاؤها، مما يقلل بشكل كبير من فرص تنفيذ المحتوى الضار من مصادر غير مصرح بها .

- **حملة مرتبطة بـBlack Basta تنشر برامج خبيثة منSystemBCعبر الهندسة الاجتماعية:**

كشفت شركة Rapid7 عن حملة هندسة اجتماعية مرتبطة بمجموعة برامج الفدية .Black Basta يستخدم المهاجمون مكالمات تقنية ومعلومات مزيفة و Microsoft Teamsلخداع المستخدمين لتثبيتAnyDesk، الذي يقوم بعد ذلك بتوصيل البرامج الضارة .تهدف هذه الحملة إلى سرقة بيانات الاعتماد واستخراج البيانات، مما يسلط الضوء على المخاطر المستمرة لهجمات التصيد الاحتيالي المعقدة[17] .

لمكافحة هجمات التصيد الاحتيالي هذه والهندسة الاجتماعية المتزايدة التعقيد والتي تم تفصيلها في سابقاً، يجب على الشركات تنفيذ أدوات مسح البريد الإلكتروني التي تمنع المرفقات والروابط الضارة قبل وصولها إلى الموظفين. يمكن تحسين أنظمة الكشف من خلال تحليل حركة المرور على الشبكة لتحديد ومنع عمليات نقل البيانات غير الطبيعية التي بدأت بواسطة برامج سطح المكتب البعيد غير المصرح بها. يساعد التدقيق والتحكم بانتظام في الوصول إلى البيانات الحساسة باستخدام الاتصالات المشفرة في الحماية من محاولات سرقة بيانات الاعتماد أثناء هذه الهجمات. يمكن للشهادات تأمين اتصالات البريد الإلكتروني عن طريق تشفير الرسائل والتأكد من إمكانية الوصول إليها من قبل المستلم المقصود فقط، وبالتالي منع سرقة بيانات الاعتماد عبر البريد الإلكتروني.

- **أزمة شاشة الموت الزرقاء (BSOD) في نظام التشغيل Windows :**[19]

تسبب تحديث معيب من مزود الأمن السيبرانيCrowdStrikeفي حدوث مشكلات واسعة النطاق تتعلق بشاشة الموت الزرقاء (BSOD) لأجهزة الكمبيوتر التي تعمل بنظام Windows في جميع أنحاء العالم. أثرت المشكلة على البنوك وشركات الطيران ومذيعي التلفزيون وغيرها من الشركات،

مما أجبر أجهزة الكمبيوتر والخوادم المتضررة على الدخول في حلقة تمهيد استرداد. حددتCrowdStrikeالمشكلة على أنها عيب في تحديث محتوى واحد لمضيفي Windows ونشرت إصلاحًا، لكن حل المشكلة للأجهزة المتضررة يتطلب تدخلًا يدويًا من مسؤولي تكنولوجيا المعلومات.

للتخفيف من مخاطر مثل هذه الحوادث، يمكن للشركات استخدام أنظمة تعمل على أتمتة النسخ الاحتياطي للبيانات والتكوينات الأساسية، مما يضمن إمكانية العودة بسرعة إلى الحالات التشغيلية حتى في مواجهة الاضطرابات الكبيرة. بالإضافة إلى ذلك، فإن استخدام الأدوات التي تسمح للمسؤولين بإدارة التحديثات والتصحيحات عن بُعد وبشكل مركزي يمكن أن يساعد في منع نشر البرامج المعيبة عبر شبكة واسعة من الأجهزة.

- **برنامج الفدية Dark Angels يحقق رقمًا قياسيًا جديدًا بدفع فدية قدرها 75 مليون دولار :**[17]

تلقت عصابة برامج الفدية Dark Angels مبلغ فدية قياسيًا قدره 75 مليون دولار من شركة .Fortune 50يتجاوز هذا المبلغ الرقم القياسي السابق البالغ 40 مليون دولار الذي دفعته شركة التأمين العملاقةCANبعد هجوم برامج الفدية Evil Corp . تستخدمDark Angels ، التي تم إطلاقها في 2022، استراتيجية"Big Game Hunting" ، حيث تستهدف الشركات ذات القيمة العالية للحصول على مدفوعات ضخمة بدلاً من مهاجمة العديد من الأهداف الأصغر.

استجابة للتهديدات المتصاعدة التي تشكلها مجموعات برامج الفدية مثلDark Angels ، يجب على المؤسسات اعتماد نهج أمني متعدد الطبقات يشتمل على تدابير وقائية وتفاعلية. من خلال الاستفادة من تقنيات التشفير لتأمين البيانات الحساسة واستخدام نظام نسخ احتياطي آلي صارم يسهل التعافي السريع من فقدان البيانات. يمكن أن يؤدي تنفيذ ضوابط وصول صارمة تتطلب التحقق القوي من هوية المستخدم قبل منح الوصول إلى الأنظمة الحرجة إلى منع الوصول غير المصرح به والحد من انتشار برامج الفدية داخل الشبكة.

- **مجموعة APT10الصينية تستهدف الشركات اليابانية ببرامج LODEINFO و NOOPDOORالخبيثة:**[18]

كشفت شركةCybereasonعن حملة تجسس إلكتروني مطولة أطلق عليها اسم"Cuckoo Spear" تستهدف المنظمات اليابانية. وتستخدم الحملة، المنسوبة إلى مجموعة APT10 الصينية، عائلات من البرامج الضارة مثل LODEINFO و NOOPDOORلجمع معلومات حساسة من المضيفين المخترقين. وفي بعض الحالات، حافظت الجهات الفاعلة المهددة على استمرارها داخل البيئات المستهدفة لمدة تتراوح بين عامين وثلاثة أعوام، مما يسلط الضوء على الطبيعة الخفية لعملياتها .

للدفاع ضد حملات التصيد الاحتيالي المتطورة التي تنشر برامج ضارة مثل LODEINFO وNOOPDOOR، تحتاج المؤسسات إلى تعزيز بروتوكولات أمان البريد الإلكتروني وتنفيذ مراقبة صارمة لجميع حركة المرور على الشبكة. إن تنفيذ الشهادات الرقمية التي تصادق على مرسلي البريد الإلكتروني يمكن أن يقلل بشكل كبير من حالات التصيد الاحتيالي من خلال التحقق من هوية المرسل، وبالتالي منع رسائل البريد الإلكتروني الضارة من الوصول إلى أهدافها المقصودة.

الفصل الثالث

الإطار العملي للدراسة

3-1- قراءة في استراتيجية الأمن السيبراني في سورية 2023

اعتمدت الحكومة في الجمهورية العربية السورية الاستراتيجية الوطنية للتحول الرقمي للخدمات الحكومية الإلكترونية عام 2021 . تسعى الحكومة من خلال هذه الاستراتيجية إلى تطوير قدراتها في مجال الأمن السيبراني بهدف تعزيز مستوى حماية الأصول المعلوماتية من المخاطر السيبرانية الداخلية والخارجية والتي يمكن أن تؤثر بشكل كبير على مقدرات الدولة. حيث ترسم هذه الوثيقة التوجهات الوطنية الأساسية وإطار العمل المرجعي للعاملين والمهتمين في مجال الأمن السيبراني من القطاعين العام والخاص، بما يضمن حماية الأصول المعلوماتية وفقاً لأهميتها، ويضمن توزيع الأدوار وتحديد الصلاحيات بين جميع الأطراف. [21]

أهداف استراتيجية الأمن السيبراني في سورية:

1- تأسيس بنية أمن سيبراني قوية ومستدامة توفر الحماية المتكاملة للأصول المعلوماتية والتقنية.

2- إدارة فعالة ومتكاملة لمواجهة التهديدات والتصدي للمخاطر.

3- تطوير الجوانب التشريعية والتنظيمية، ووضع القواعد القانونية الملائمة، والإجراءات المتبعة للتصدي للجرائم الخاصة بالأمن السيبراني.

4- تطوير وصقل الإمكانات الوطنية، البشرية والتقنية للأمن السيبراني، وبناء الثقافة وإذكاء الوعي المجتمعي للوصول لأفضل الممارسات في مجال الأمن السيبراني.

5- تشجيع الأبحاث والتحقيقات والبحث العلمي في مجال الأمن السيبراني.

6- تحقيق الحوكمة الفعالة للتنسيق بين جميع الجهات وضمان حُسن التنفيذ.

7- تعزيز التنسيق والتعاون في قضايا الأمن السيبراني على المستويين الإقليمي والدولي.

انبثق عن استراتيجية الأمن السيبراني ستة برامج، هي:

البرنامج الأول:أمن البنى التحتية

يهدف هذا البرنامج إلى دعم الشبكة والنظم المعلوماتية الوطنية بالحلول الأمنية العتادية والبرمجية والتصميمية لزيادة مناعتها في مواجهة الهجمات الإلكترونية. يتضمن هذا البرنامج إنشاء وتطوير المركز الوطني للاستجابة للطوارئ المعلوماتية، وتأهيل فريق مختص بتكنولوجيا المعلومات وأمنها للاستجابة للطوارئ المعلوماتية، وتشكيل فرق للاستجابة للطوارئ المعلوماتية في المؤسسات التي لديها منظومات معلوماتية، واستكمال بناء منظومة التوقيع الرقمي، بالإضافة إلى تعزيز البنية التحتية المعلوماتية للمؤسسات التي لديها منظومات معلوماتية.

البرنامج الثاني: تطوير الإطار القانوني والتنظيمي

يهدف هذا البرنامج إلى مراجعة الجوانب القانونية والتنظيمية المتعلقة بالأمن السيبراني من قوانين وسياسات وضوابط والوصول إلى إصدار تشريع للأمن السيبراني بعد مراجعة شاملة لكافة القوانين ذات الصلة بالأمن السيبراني، وقانون حماية البيانات الشخصية. حيث صدر القانون رقم 7 لعام 2023 المتضمن إحداث "الهيئة الوطنية لخدمات تقانة المعلومات" لتحل محل "الهيئة الوطنية لخدمات الشبكة" بهدف مواكبة التقدم والتطور الحاصل في مجال خدمات الإنترنت والاستضافة، ودعم الصناعة البرمجية الوطنية، وتنظيم خدمات التوقيع الرقمي والبطاقة الالكترونية متعددة المهام، وتحقيق أمن المعلومات في ظل الانتشار الكبير للتطبيقات الذكية.وتضمن القانون مهام للهيئة الجديدة بمنحها الحق الحصري لتقديم خدمات أمن المعلومات للجهات العامة والإشراف على تحقيق متطلبات أمن المعلومات في القطاع الخاص، كما وضع عقوبات جديدة وشدد العقوبات السابقة بغية ضبط العمل في مجال عمل الهيئة، وضمان حسن الالتزام بالضوابط الصادرة عنها.

البرنامج الثالث: نشر ثقافة الوعي السيبراني

يهدف هذا البرنامج إلى تعزيز الوعي العام للمستخدمين بالقضايا الأساسية المتعلقة بالأمن السيبراني، حيث تم تحديد خمسة مسارات رئيسية لعمل البرنامج تتمثلبتعزيز الوعي بقضايا الأمن السيبراني، والثقة لدى المستخدمين تجاه الخدمات المقدمة على الشبكة، ورفع مستوى فهم المستخدمين لأهمية حماية بياناتهم علىالشبكة، ووضع آلية لإدارة ومعالجة الشكاوى المتعلقة بالاستخدامات المسيئة على

شبكة الإنترنت، والاعتماد على وسائل الإعلام والمنصات الإعلامية الرقمية فيتغطية القضايا المتعلقة بالأمن السيبراني.

البرنامج الرابع: بناء القدرات والمعرفة

يهدف هذا البرنامج إلى تنمية القدرات في مجال الأمن السيبراني لدى الحكومة والقطاع الخاص والمواطنين بشكل عام، وذلك وفق ثلاث مسارات رئيسية هي:

1- التعليم في مجالات الأمن السيبراني

2- التدريب الاحترافي في مجالات الأمن السيبراني.

3 –البحث والابتكار في مجالات الأمن السيبراني.

حيث تم تنفيذ عدد من الدورات التدريبية للعاملين في مجال تقانة المعلومات وأمن المعلومات من القطاعين العام والخاص وذلك في مركز (التميز السوري- الهندي) بدمشق الذي افتتح عام 2011، حيث تجاوز عدد الدورات المنفذة خلال عامي(2022-2023) 17 دورة استفاد منها 326 متدرباً منهم مهندسون وفنيون.

البرنامج الخامس: الشراكات والتعاون الإقليمي والدولي

يهدف البرنامج إلى تطوير الشراكات والتعاون على المستويين الإقليمي والدولي في مجال الأمن السيبراني، بما يسمح بتبادل الخبرات والإنذار المبكر حول الأخطارالمحتملة والحوادث الأمنية الشائعة، ووضع آليات للتصدي لهذه الحوادث وخطة لمعالجتها من خلال مراكز الاستجابة للطوارئ المعلوماتية، وصولاًإلى إيجاد اتفاقاتدولية وعربية في مجال مكافحة الجرائم الإلكترونية، وتعزيز دور القطاع الخاص المحلي في مجال الأمن السيبراني، بما يساهم في دعم الجهود الوطنية الرامية إلىرفع مستوى أمن المعلومات في القطاعين العام والخاص.

البرنامج السادس: تطوير هياكل وظيفية متخصصة

تخصيص وحدات هيكلية تُعنى بالأمن السيبراني في كل جهة عامة ضرورة ملحة، مع تأمين المستلزمات الفنية والكوادر البشرية المؤهلة والمدربة والتي تسهمفي تنفيذ الاستراتيجية المقرة من الحكومة.

3-2- تخطيط الجزء العملي في ضوء الاستراتيجية الوطنية للأمن السيبراني

سعينا في هذا البحث إلى المضي في ضوء الاستراتيجية الوطنية للأمن السيبراني حيث قمنا في القسم النظري بتسليط الضوء على مفاهيم الأمن السيبراني والقضايا المتعلقة بها، وهذا يتوافق مع الهدفين (4) و (5) للاستراتيجية. أما في القسم العملي فإننا سنسعى إلى التوافق مع البرنامج الثالث المنبثق عن الاستراتيجية (نشر ثقافة الوعي السيبراني)، حيث سنقوم بقياس مستوى الوعي الاجتماعي لمخاطر الأمن السيبراني من خلال نشر استبيان الكتروني بين طلبة الجامعات.

3-3- قياس مستوى الوعي الاجتماعي في سورية لمخاطر الأمن السيبراني

جرى تصميم استبيان الكتروني موجّه إلى طلبة الجامعات السورية، وهم الفئة الأكثر استخداماً وتعمقاً في الفضاء السيبراني. يهدف الاستبيان إلى اختبار فرضيات البحث وأهمها البحث عن علاقة الوعي لقضايا الأمن السيبراني بمستوى التعليم ونوع التخصص والعمر، وكذلك أهمية برامج التوعية السيبرانية ومخاطر الاستخدام المتزايد لوسائل التواصل الاجتماعي.

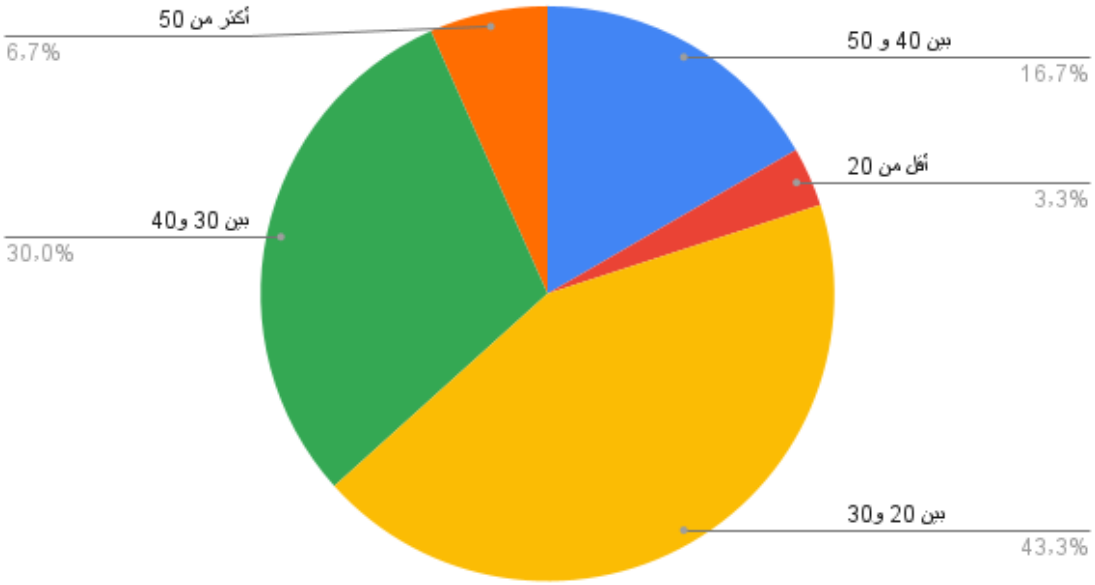
احتوى الاستبيان على 19 سؤال، قمنا بتقسمها إلى أربعة مجموعات.

المجموعة الأولى: طرح الاستبيان أربعة أسئلة للتعرف على العينة، وهي مبينة في الجدول التالي:

م	السؤال	الأجوبة
1	ما عمرك؟	أقل من 20 سنة بين 20 و30 بين 30 و40 بين 40 و 50 أكثر من 50
2	ماهي الشهادة التي تحملها؟	ثانوية- جامعية- ماجستير- دكتوراة
3	ماهو تخصصك الدراسي؟	علوم تقنية - علوم إنسانية
4	هل حصلت على أي تدريب حول الأمن السيبراني؟	نعم- لا

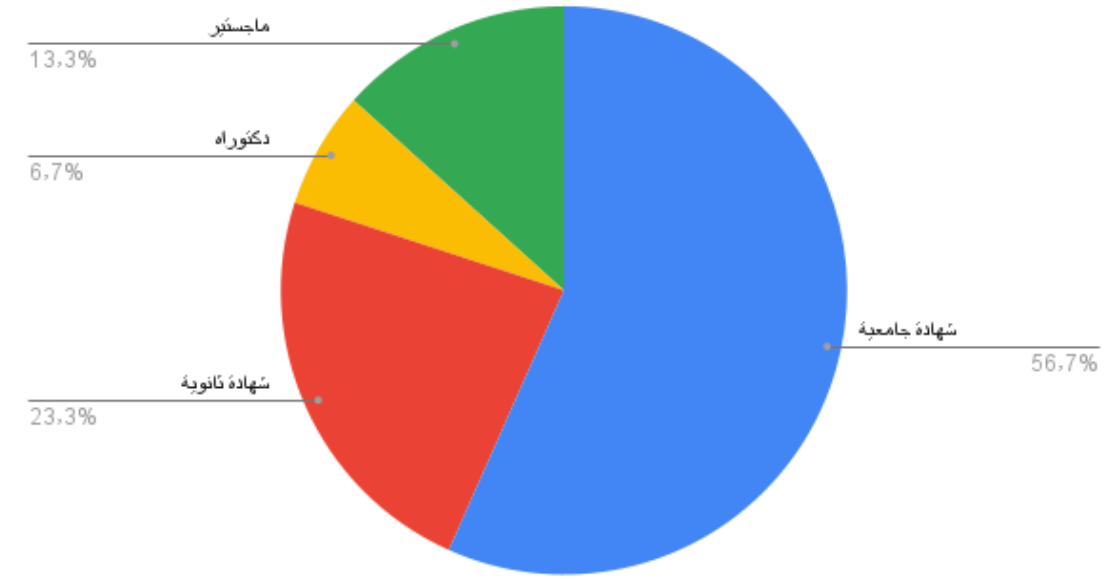
الهدف من هذه الأسئلة هو دراسة درجة الوعي للأمن السيبراني تبعاً لهذه المتغيرات المستقلة، حيث سنقوم بقياس درجة الوعي في مجموعة أسئلة لاحقة.

بتحليل نتائج الأجوبة تبين أن غالبية العينة (73.3% كما هو موضح بالشكل 3-1) من فئات عمرية بين ال20 وال40 سنة، وهي فعلياً شريحة طلاب الجامعات.



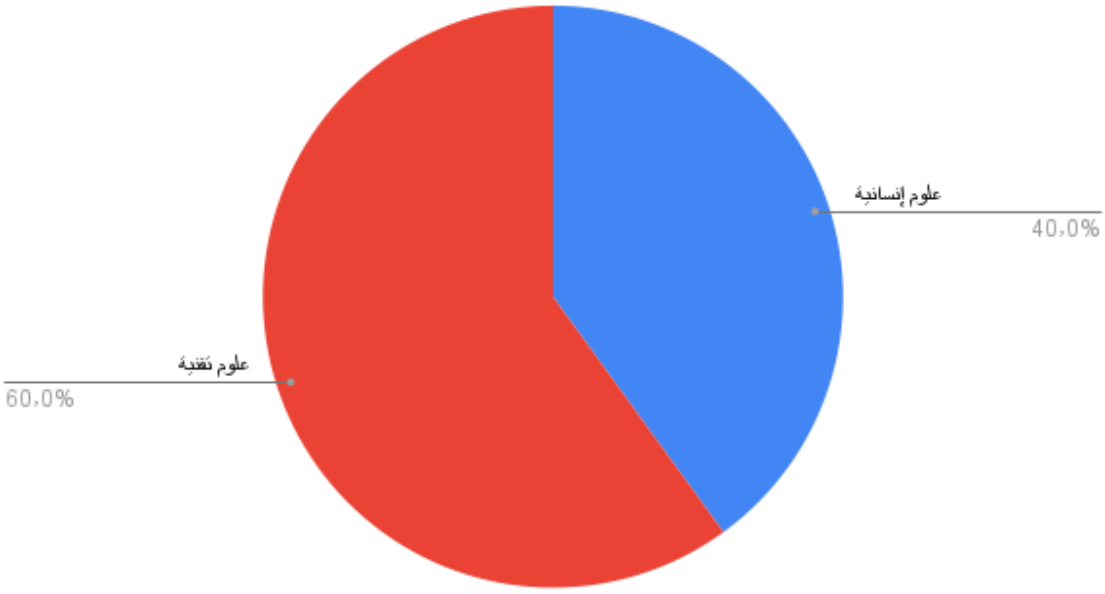
الشكل 3-1- الفئات العمرية للعينة في الاستبيان

كما تبين أن 56.7% من العينة تحمل شهادة جامعية فقط، و 23.3% تحمل شهادة ثانوية فقط، أما حملة شهادات الماجستير والدكتوراة فلم تتجاوز نسبتهم 19%. وهذا التوزع يعطي مصداقية أكبر لنتائج الاستبيان كون التوزع يشمل جميع مستويات حملة الشهادات بنسب قريبة للواقع.



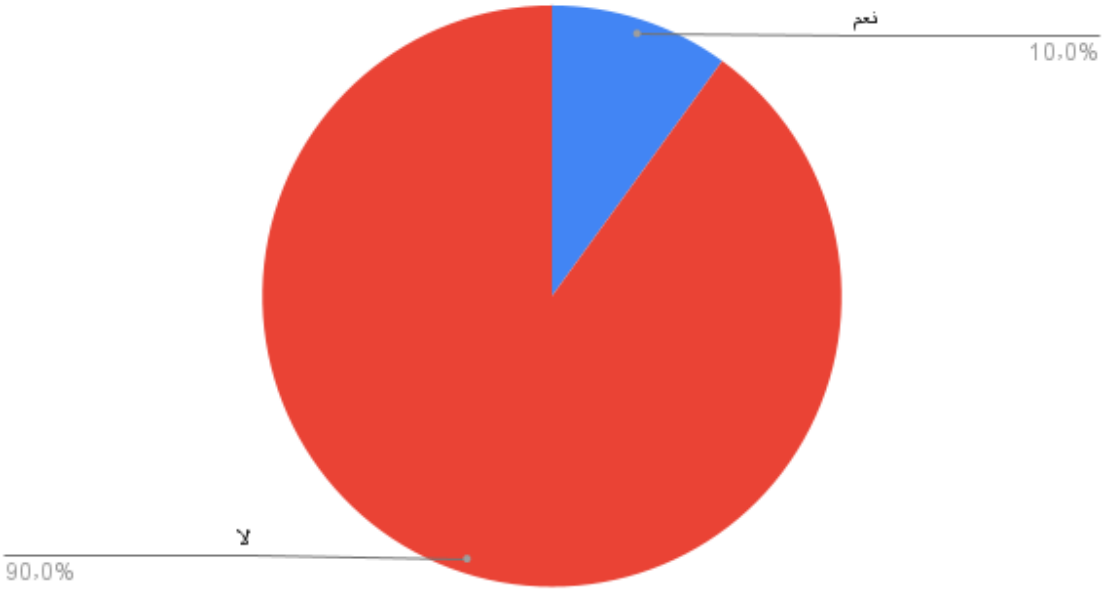
الشكل 3-2- توزع العينة من حيث الشهادة

أما من حيث نوع التخصص الدراسي فقد كانت نسبة 60% تعود للمتخصصين في المجالات التقنية (وهم من نتوقع أن يكونوا على دراية أكبر بمواضيع الأمن السيبراني)، بينما 40% تعود للمتخصصين في علوم انسانية. الشكل 3-3.



الشكل 3-3- توزع العينة من حيث نوع التخصص

كما أفاد 90% من العينة أنهم لم يتلقوا أي تدريب حول الأمن السيبراني (الشكل 3-4). وهذا يشير إلى نقص التدريب المتاح في الجامعات في مجال الأمن السيبراني.

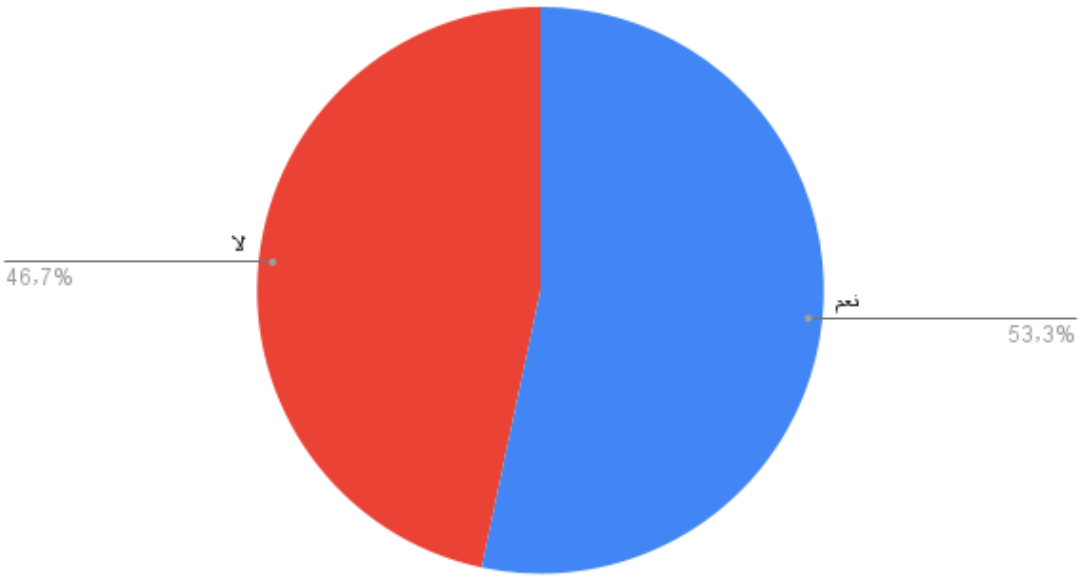


الشكل 3-4- توزع العينة من حيث حصولهم على تدريب حول الأمن السيبراني

المجموعة الثانية: طرح الاستبيان خمسة أسئلة للتعرف على أهمية الأمن السيبراني من وجهة نظر العينة. يبين الجدول التالي هذه الأسئلة:

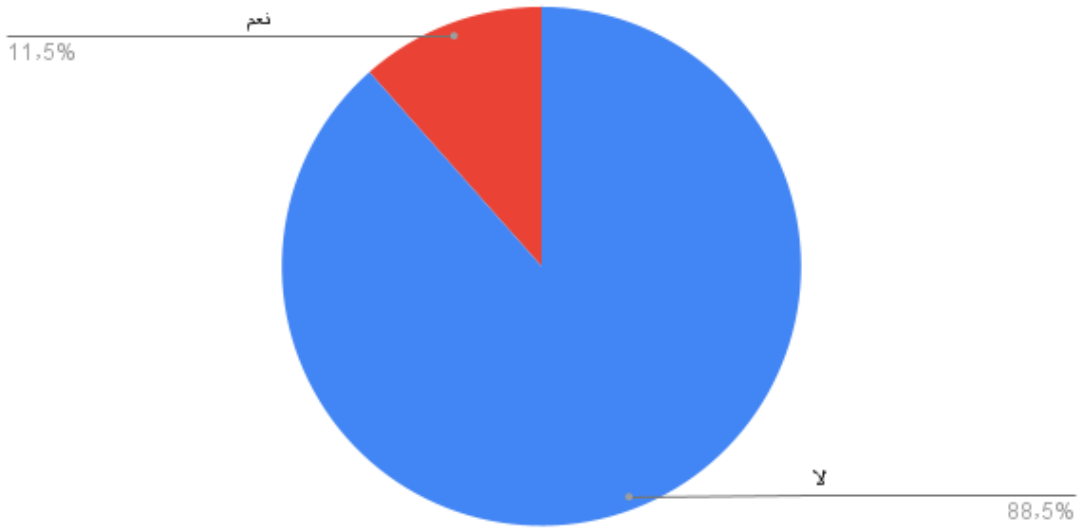
م	السؤال	الأجوبة
1	هل لديك معرفة بمفهوم الأمن السيبراني؟	نعم- لا
2	هل أنت على دراية بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في الجمهورية العربية السورية؟	نعم- لا
3	كيف تقيم أهمية الأمن السيبراني في حياتك الشخصية والمهنية؟	مهمة جداَ- مهمة - غير مهمة
4	هل تعتقد أن لديك مهارات كافية لاكتشاف الرسائل الاحتيالية؟	نعم–لا–ربما
5	هل تعتقد أن لديك معلومات كافية حول كيفية حماية نفسك من التهديدات السيبرانية؟	نعم–لا–ربما

بتحليل نتائج الاستبيان تبين أن العينة توزعت بشكل متساوي تقريباً بين من يعتقدون أنهم على دراية كافية بمفاهيم الأمن السيبراني (53.3%) وبين من يقرّون بجهلهم بهذه المفاهيم (46.7%). الشكل (3-5).



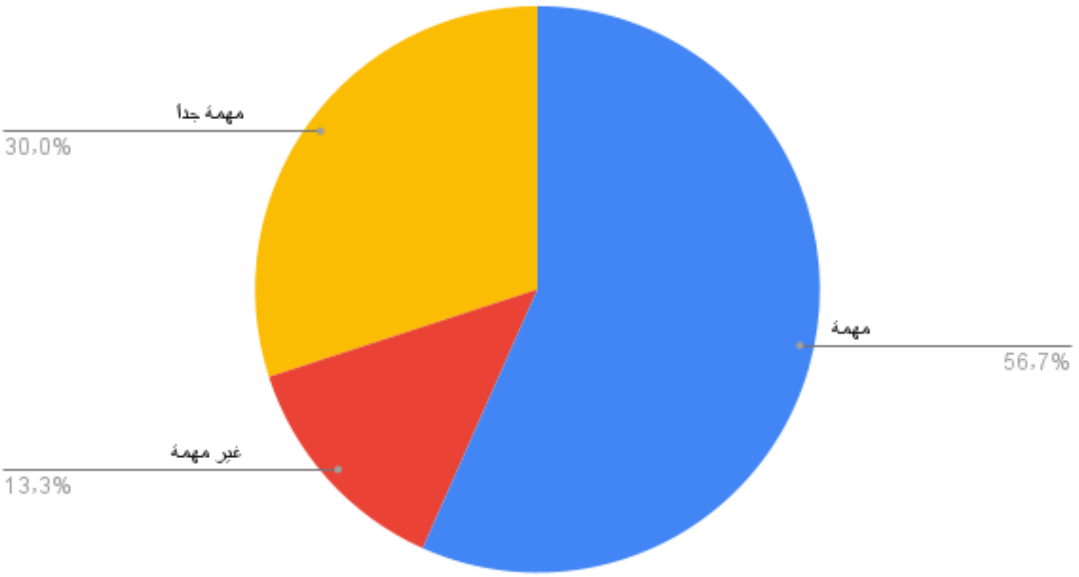
الشكل 3-5- توزع العينة من حيث نظرتهم لأنفسهم حول المعرفة بالأمن السيبراني

وعند طرح سؤال معرفة أفراد العينة بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في الجمهورية العربية السورية، أفادت الأغلبية (88.5%) بجهلهم بهذه القوانين مما يشير إلى فجوة في ينبغي معالجتها من خلال ورش عمل أو محاضرات توعوية، وقد تكون هذه الفجوة مبررة نظراً لحداثة هذه القوانين. الشكل (3-6).



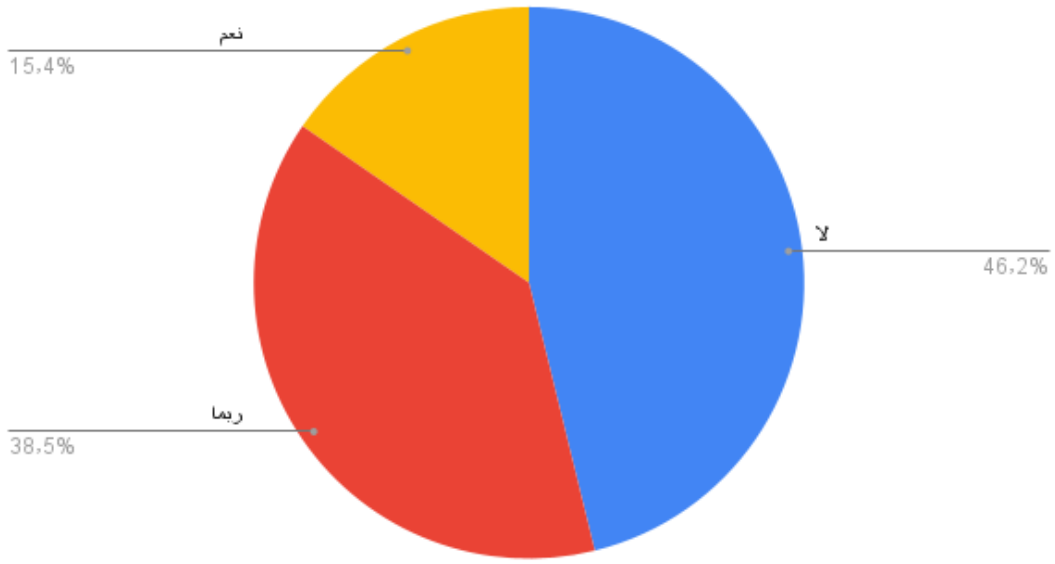
الشكل 3-6- نتائج استبيان فيما إذا كانت العينة على دراية بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في سورية

من ناحية أهمية الأمن السيبراني في حياة أفراد العينة، اتفقت غالبية العينة (83.7%) على أنها مهمة أو مهمة جداً، بينما رأت نسبة قليلة 13.3% أنها غير مهمة. الشكل (3-7). تعكس هذه النتيجة وعيًا عامًا يحتاج إلى تعزيز لتأكيد أهميتها.

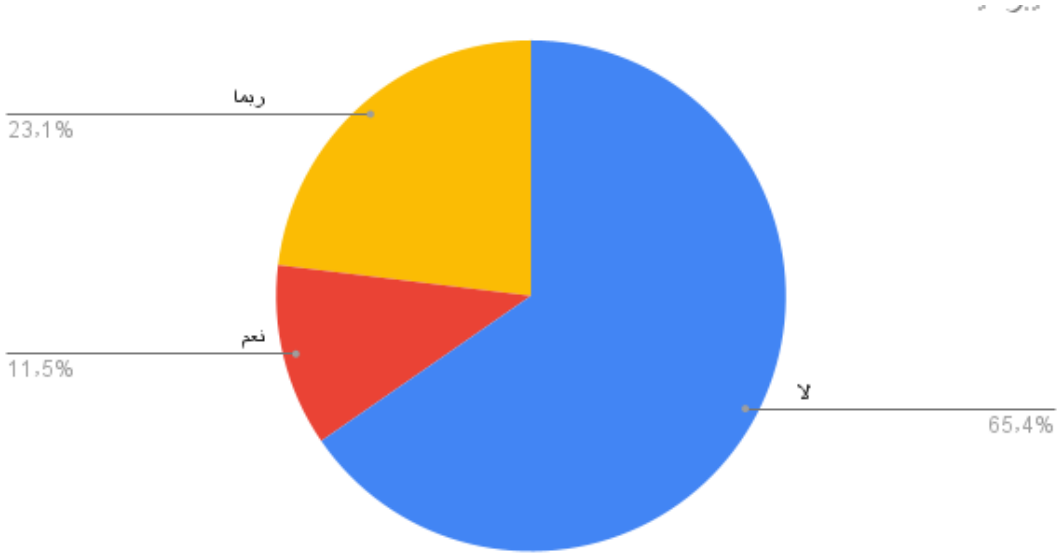


الشكل 3-7- أهمية الأمن السيبراني من وجهة نظر العينة

من ناحية المهارات والمعلومات الكافية حول التعامل مع التهديدات السيبرانية، أكدت غالبية العينة عدم امتلاكها لهذه المهارات، أو تشككت على الأقل في ذلك. أما النسبة التي تعتقد أن لديها هذه المهارات فلم تتجاوز 15% كما هو موضح بالشكل 3-8 والشكل 3-9. و تشير هذه النتائج إلى نقص التعليم والتدريب في هذا المجال.



الشكل 3-8- امتلاك أفراد العينة لمهارات اكتشاف الرسائل الاحتيالية (من وجهة نظرهم)

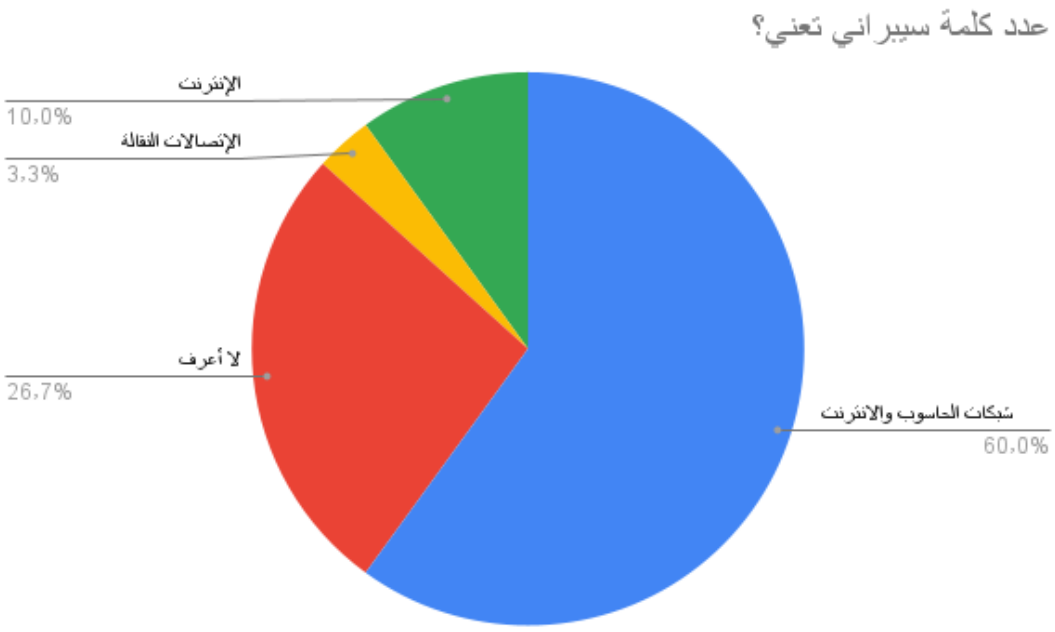


الشكل 3-9- امتلاك أفراد العينة لمهارات الحماية من التهديدات السيبرانية (من وجهة نظرهم)

المجموعة الثالثة: طرح الاستبيان سبعة أسئلة لاختبار وقياس المستوى الحقيقي لوعي العينة للأمن السيبراني.

م	السؤال	الأجوبة
1	كلمة سيبراني تعني؟	▪ شبكات الحاسوب والانترنت والاتصالات ▪ الإتصالات النقالة ▪ الإنترنت ▪ لا أعرف
2	ما حدث في لبنان من تفجير أجهزة البيجر كان؟	▪ اختراق سيبراني ▪ اختراق استخباراتي ▪ لا أعرف
3	عندما يصلني رابط إلكتروني إلى حسابي على فيسبوك فإنني؟	▪ أقوم بفتح الرابط فورًا دون تردد ▪ أبحث عن معلومات حول الرابط على الإنترنت ▪ أقوم بفتح الرابط فقط إذا كان من جهة موثوقة
4	ماذا أفعل عند وصول رسالة إلى بريدي الإلكتروني تفيد بحصولي على جائزة مالية؟	▪ أفتح الرسالة وأقرأ التفاصيل ▪ أقوم بحذف الرسالة مباشرة ▪ أقوم بإرسال الرسالة لأصدقائي للتحقق منها ▪ أتحقق من مصدر الرسالة قبل اتخاذ أي إجراء
5	هل تستخدم كلمات مرور قوية وفريدة لحساباتك الإلكترونية؟	▪ دائما ▪ أحيانا ▪ نادرا ▪ أبدا
6	هل لديك تطبيقات لمكافحة الفيروسات مثبتة على أجهزتك؟	▪ نعم ▪ لا ▪ ربما
7	هل سبق لك أن قمت بتغيير إعدادات الخصوصية في حساباتك على وسائل التواصل الاجتماعي؟	▪ نعم ▪ لا

في السؤال الأول، أجاب 60% من أفراد العينة إجابة صحيحة، ورغم بساطة هذا السؤال أخطأ 40% من أفراد العينة في الإجابة. وهذا يدل على وعي متوسط لكلمة سيبيراني. يوضح الشكل (3-10) توزع إجابات العينة على هذا السؤال.



الشكل 3-10- توزع الإجابات على السؤال الأول (مذكور أعلى الشكل)

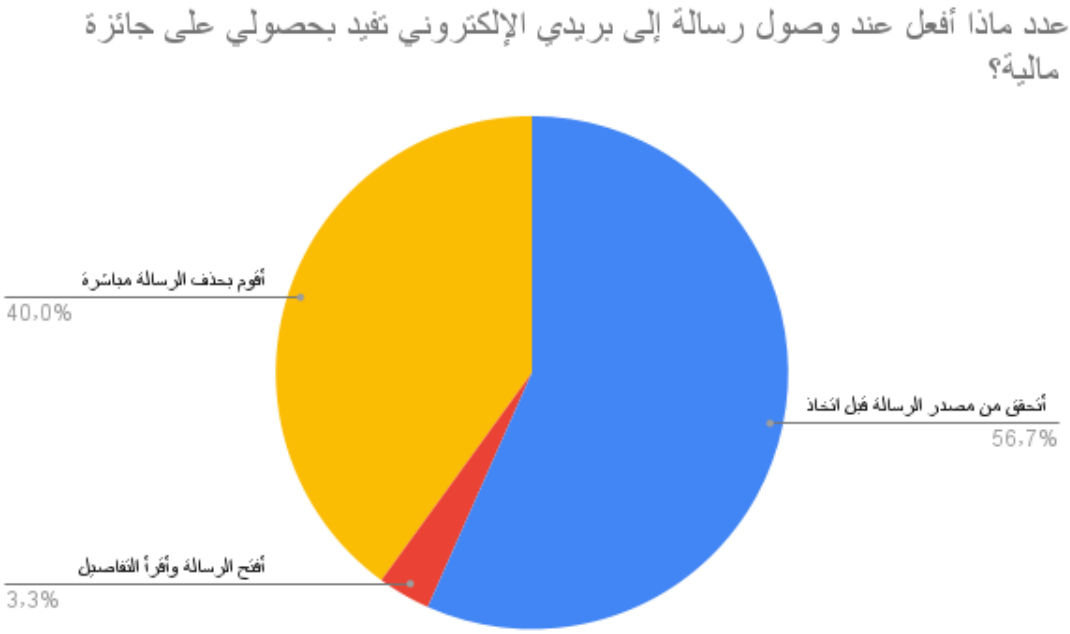
في السؤال الثاني، وهو سؤال ليس بالبسيط، توزعت إجابات أفراد العينة بالتساوي تقريباً بين الإجابات الثلاثة، أي أن نسبة الأفراد أصحاب الإجابة الصحيحة هي فقط بحدود ثلث العينة. وهذه النتيجة تعزز من الدلالة على قلة وعي أفراد العينة بمفهوم الأمن السيبيراني. يوضح الشكل (3-11) توزع إجابات العينة على هذا السؤال.

الشكل 3-11- توزع الإجابات على السؤال الثاني (مذكور أعلى الشكل)

في السؤال الثالث، أجاب 63% من أفراد العينة إجابة صحيحة، وهذا يعزى إلى كثرة استخدام وسائل التواصل الاجتماعي وكثرة تعرض الناس لهذا النوع من التهديدات السيبرانية. هذه النتيجة تعكس وعيًا جيدًا بمخاطر الروابط المشبوهة. يوضح الشكل (3-12) توزع إجابات العينة على هذا السؤال.

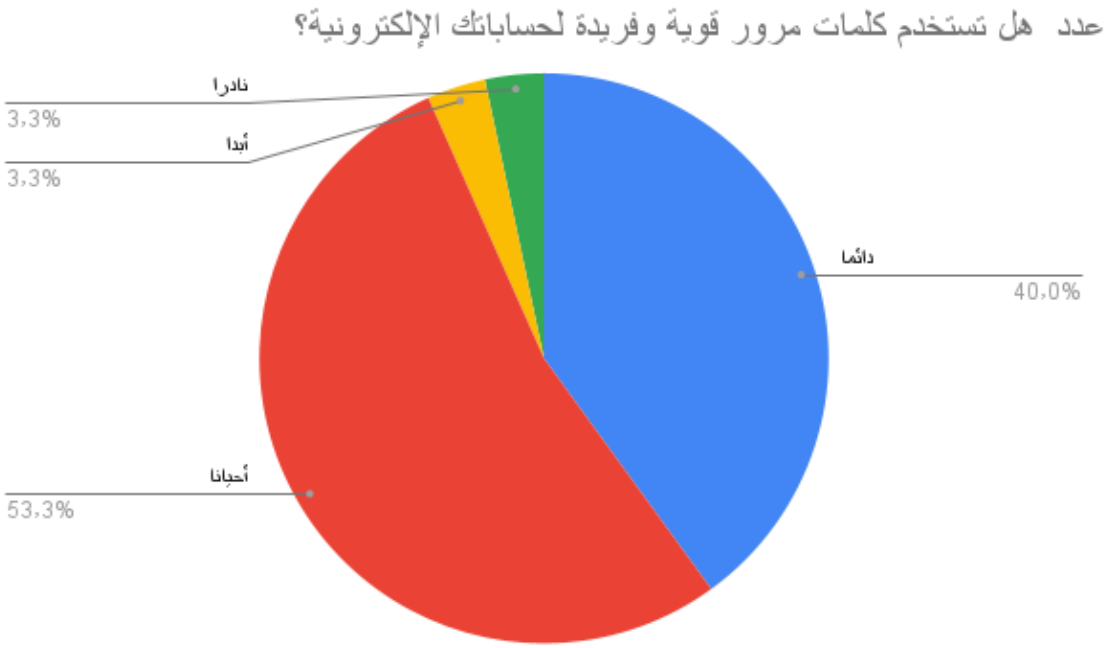
الشكل 3-12- توزع الإجابات على السؤال الثالث (مذكور أعلى الشكل)

في السؤال الرابع، الغالبية العظمى من الإجابات صحيحة، وهذا يعزى أيضاً إلى كثرة استخدام البريد الالكتروني وكثرة تعرض الناس لهذا النوع من التصيد الاحتيالي. هذه النتيجة تعكس وعيًا جيدًا بمخاطر رسائل التصيد الاحتيالي. يوضح الشكل (3-13) توزع إجابات العينة على هذا السؤال.



الشكل 3-13- توزع الإجابات على السؤال الرابع (مذكور أعلى الشكل)

في السؤال الخامس، تشير الإجابات إلى أن الغالبية العظمى من العينة متنبهة إلى أهمية استخدام كلمات مرور قوية، لكن البعض قد يرى أن حسابه ليس بهذه الأهمية لاختيار كلمة مرور قوية. يوضح الشكل (3-14) توزع إجابات العينة على هذا السؤال.



الشكل 3-14- توزع الإجابات على السؤال الخامس (مذكور أعلى الشكل)

في السؤال السادس، لا تمتلك غالبية أفراد العينة (75%) تطبيقات لمكافحة الفيروسات أو أنها لا تعرف إذا كان لديها أحد هذه التطبيقات. تعكس هذه النتائج وجود ضعف في الممارسات الأمنية بين الطلاب. يوضح الشكل (3-15) توزع إجابات العينة على هذا السؤال.

الشكل 3-15- توزع الإجابات على السؤال السادس (مذكور أعلى الشكل)

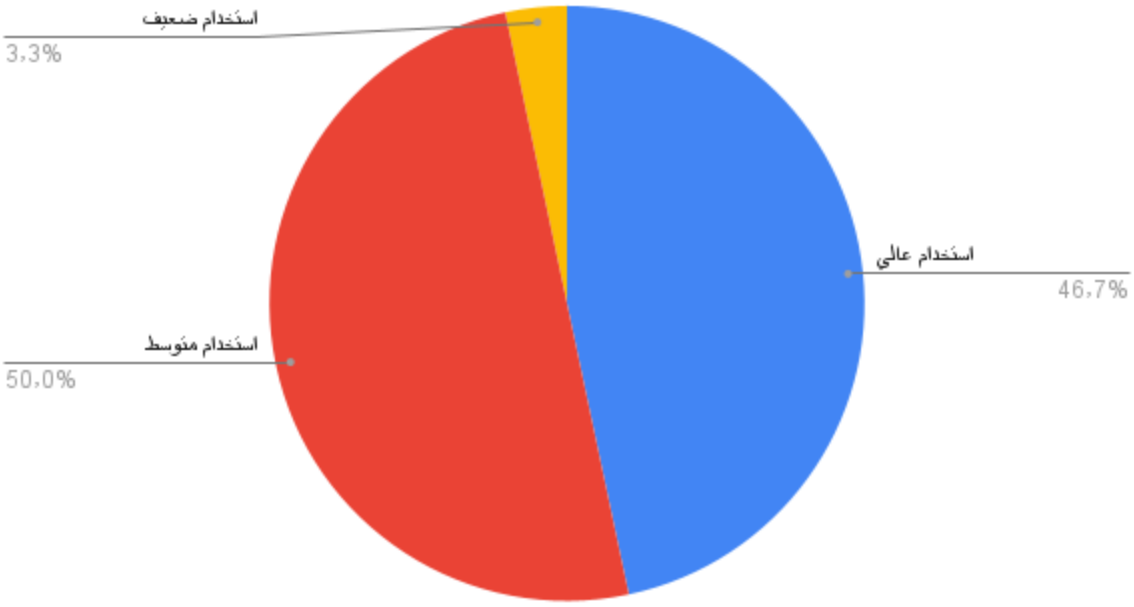
في السؤال السابع، وهو هل سبق لك أن قمت بتغيير إعدادات الخصوصية في حساباتك على وسائل التواصل الاجتماعي؟ فقاد أجاب أغلب أفراد العينة بنعم. وهذا يدل على وعي جيد للأمن السيبراني.

لدراسة العلاقة بين درجة الوعي للأمن السيبراني وبين مستوى الشهادة الجامعية والتخصص من جهة ثانية، قمنا بإعطاء علامة لكل جواب صحيح من الأسئلة السبعة في هذه المجموعة (الثالثة)، وبحيث تكون علامة كل فرد من أفراد عينة الاستبيان تتراوح بين 0 (وعي معدوم) و 7 (وعي عالي). بتحليل نتائج هذه الخطوة وجدنا أن وسطي علامات الأفراد من تخصصات تقنية هو 5.7 (من 7) بينما انخفض وسطي علامات الأفراد من تخصصات انسانية إلى 2.5، وهو ما يؤكد فرضية أن أصحاب التخصصات التقنية أكثر وعياً لمفاهيم الأمن السيبراني من أصحاب التخصصات الانسانية. وبالنظر إلى مستوى الشهادة لدى أفراد العينة من تخصصات تقانية وجدنا أن وسطي علامة من يحمل شهادة الدكتوراة كان 7، أما وسطي علامة حملة شهادة الماجستير كان 6، وانخفضت العلامة إلى 5 لحملة الشهادة الجامعية فقط.

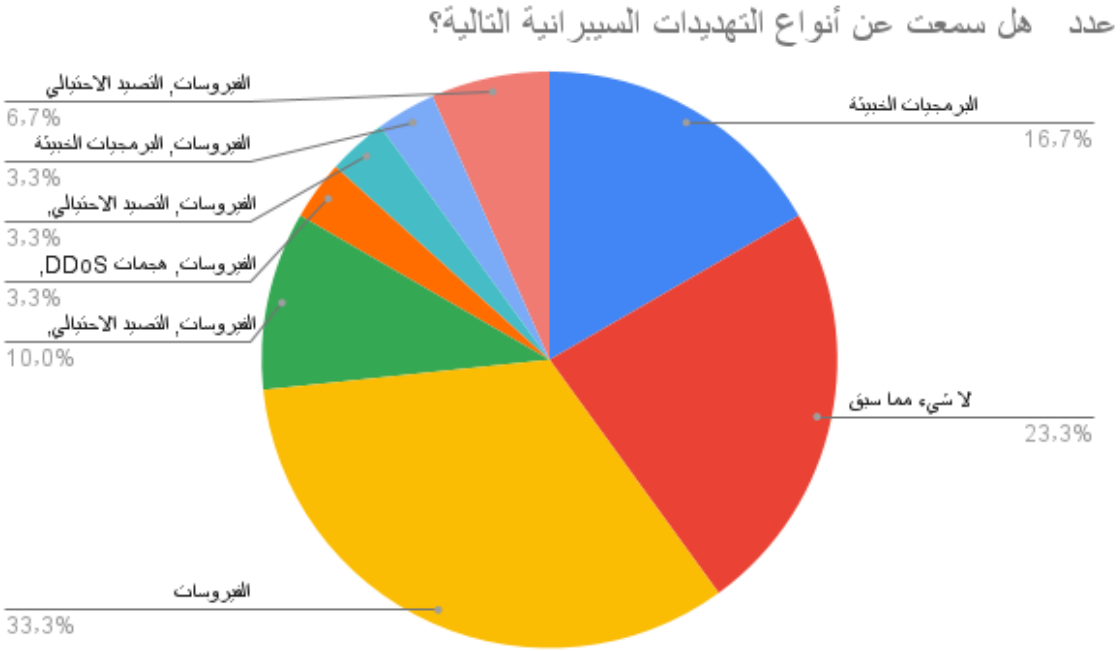
المجموعة الرابعة: طرح الاستبيان سؤالين لقياس علاقة الاستخدام المتزايد لوسائل التواصل الاجتماعي بالوعي للتهديدات السيبرانية.

م	السؤال	الأجوبة
1	ما هو مدى استخدامك لوسائل التواصل الإجتماعي؟	▪ استخدام عالي ▪ استخدام متوسط ▪ استخدام ضعيف
2	هل سمعت عن أنواع التهديدات السيبرانية التالية؟	▪ الفيروسات ▪ التصيد الاحتيالي ▪ هجماتDDoS ▪ البرمجيات الخبيثة ▪ لا شيء مما سبق

هدف هذه المجموعة من الأسئلة إلى الربط بين تزايد استخدام وسائل التواصل الاجتماعي وبين زيادة التعرض لهجمات سيبرانية. يبين الشكلين التاليين نتائج الإجابات على هذه المجموعة من الأسئلة.



الشكل 3-16- توزع الإجابات على سؤال ما مدى استخدامك لوسائل التواصل الاجتماعي



الشكل 3-17- توزع الإجابات على أنواع التهديدات السيبرانية التي تعرضت لها العينة

يتضح أن غالبية أفراد العينة يستخدمون وسائل التواصل الإجتماعي بشكل كبير أو متوسط، ونلاحظ أن غالبية أفراد العينة بنسبة 76.7% قد واجهت تهديدات سيبرانية، كان أكثرها الفيروسات، تليها البرمجيات الخبيثة، ثم التصيد الاحتيالي.

السؤال الأخير:هل لديك أي اقتراحات لتحسين الوعي الأمني بالمخاطر السيبرانية بين الطلبة في الجامعات السورية؟ (اختياري)

جاءت ردود قليلة على هذا السؤال، بعضها وجدناه مفيداً، ونوجزه كالتالي:

- تدريس مقررات الأمن السيبراني واعتبارها مادة اساسية
- إقامة ندوات ومحاضرات وورشات تدريبية تشرح أمن المعلومات والاتصالات والأمن السيبراني، وماهي التهديدات السيبرانية للأجهزة الحديثة، وكيفية حماية الحسابات الشخصية واساليب التصيد الاحتيالي و تجنبها.

3-4- ملخص نتائج الاستبيان

تم إجراء استبيان بين طلبة الجامعات يهدف إلى سبر مفهوم وإجراءات الأمن السيبراني لدى الطلاب.

كانت غالبية العينة من فئات عمرية بين ال20 وال40 سنة، وهي فعلياً شريحة طلاب الجامعات. وقد توزعت الشريحة ما بين حملة الثانوية فقط (طالب جامعي) وما بين حملة الإجازة والماجستير والدكتوراة. وهذا التوزع يعطي مصداقية أكبر لنتائج الاستبيان كون التوزع يشمل جميع مستويات حملة الشهادات بنسب قريبة للواقع. أما من حيث نوع التخصص الدراسي فقد توزعت العينة بشكل متقارب بين المتخصصين في المجالات التقنية (وهم من نتوقع أن يكونوا على دراية أكبر بمواضيع الأمن السيبراني)، وبين المتخصصين في العلوم الانسانية.

اتفقت الغالبية العظمى من العينة على أهمية مفاهيم الأمن السيبراني، لكنها لم تتلق أي تدريب حول الأمن السيبراني، وهذا يشير إلى نقص التدريب المتاح في الجامعات في مجال الأمن السيبراني، كما

يظهر أن معرفتهم بتهديدات الأمن السيبراني جاءت غالبًا من التجارب الشخصية مثل تعرض الحواسيب التي يعملون عليها لوجود فيروسات.. كما أبدت عينة الاستبيان جهلاً واضحاً بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في الجمهورية العربية السورية، مما يشير إلى فجوة ينبغي معالجتها من خلال ورش عمل أو محاضرات توعوية (وقد تكون هذه الفجوة مبررة نظراً لحداثة هذه القوانين).

توزعت العينة بشكل متساوي تقريباً بين من يعتقدون أنهم على دراية كافية بمفاهيم الأمن السيبراني وبين من يقرّون بجهلهم بهذه المفاهيم. وعند وضع أفراد العينة تحت الاختبار عن طريق طرح أسئلة تسبر فهمهم الحقيقي للمفاهيم السيبرانية تبين وجود فهم متوسط لهذه المفاهيم وضعف وعي لها. وقد عادت هذه النتيجة لتتعزز عندما أكد أغلب أفراد العينة أنهم لا يرون أنفسهم مؤهلين للتعامل مع التهديدات السيبرانية.

ونظراً لكثرة استخدام أفراد العينة لمواقع التواصل الاجتماعي والبريد الإلكتروني، فقد ازدادت نسبة تعرضهم للتهديدات السيبرانية (كان أكثرها الفيروسات، تليها البرمجيات الخبيثة، ثم التصيد الاحتيالي)، ولذلك فقد لمسنا منهم وعيًا جيدًا بمخاطر التصيد الاحتيالي والروابط المشبوهة، كما لمسنا منهم وعياً مرتفعاً إلى أهمية استخدام كلمات مرور قوية، وتغيير إعدادات الخصوصية في حسابات مواقع التواصل الاجتماعي. لكن البعض رأى أن حساباته ليس بهذه الأهمية لاختيار كلمة مرور قوية، وهذه الرؤية عادت للظهور عند السؤال عن استخدام تطبيقات مكافحة الفيروسات إذ أقرت غالبية أفراد العينة بأنها لا تمتلك تطبيقات لمكافحة الفيروسات أو أنها لا تعرف إذا كان لديها أحد هذه التطبيقات.

الفصل الرابع

النتائج والتوصيات

4-1- النتائج

هدف هذا البحث إلى الإضاءة على مفاهيم الأمن السيبراني، وتحليل التهديدات السيبرانية الحديثة، وتقييم فعالية استراتيجيات الأمن السيبراني، ومدى الوعي بين طلاب الجامعات لمخاطر الأمن السيبراني. وقد غطى القسم النظري للبحث المفاهيم النظرية الأساسية ثم انتقلنا في القسم العملي إلى تنفيذ الدراسة الاستكشافية بين طلبة الجامعات.

أظهرت الدراسة الاستكشافية حول مدى الوعي الأمني بالمخاطر والتهديدات السيبرانية بين طلبة الجامعات في سورية أن الوعي لهذه المخاطر متوسط عموماً. ويبدو أن الطلبة يعتمدون على وسائل التواصل الاجتماعي والمقالات الإلكترونية كمصادر رئيسية للمعلومات، مما يعكس الحاجة إلى توجيههم نحو مصادر أكثر موثوقية عبر البرامج التعليمية والتدريب.

أظهرت نسبة كبيرة من الطلبة معرفة بنوع محدد من التهديدات السيبرانية وهو الفيروسات، بينما كانت المخاطر المرتبطة بالأنواع الأخرى كالتصيد الاحتيالي وهجوم Ddos أقل شهرة.

بالإضافة إلى ذلك، شعرت الغالبية العظمى من العينة بعدم ثقة في قدرتها على التعامل مع الهجمات السيبرانية، مما يستدعي تعزيز المهارات العملية والتدريب في هذا المجال. وظهرت جلياً فجوة الإعلام والتعليم عندما أبدى الغالبية من العينة جهلهم بالتشريعات والقوانين المتعلقة بالجرائم السيبرانية في الجمهورية العربية السورية.

4-2- التوصيات

يمكن في نهاية هذا البحث تقديم التوصيات التالية:

- ضرورة إدراج مناهج تعليمية متخصصة في الأمن السيبراني ضمن البرامج الدراسية الجامعية.
- تنظيم ورش عمل ودورات تدريبية لرفع مستوى الوعي والمهارات لدى الطلبة.
- إقامة ندوات ومحاضرات وورشات تدريبية تشرح أمن المعلومات والاتصالات والأمن السيبراني، وماهي التهديدات السيبرانية للأجهزة الحديثة، وكيفية حماية الحسابات الشخصية واساليب التصيد الاحتيالي و تجنبها.
- تعزيز التعاون بين الجامعات ووزارة الاتصالات والتقانة لتوفير موارد تعليمية موثوقة في في مجال الأمن السيبراني.

المراجع

1- متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود .د.منى عبد الله السمحان- جامعة الملك سعود -المملكة العربية السعودية-2020

2- العلوم التربوية والنفسية وعلاقتها بالأمن السيبراني. الدكتور معتصم تركي الضالعين – مجلة الشرق الأوسط للنشر العلمي 14-1-2024

3- الأمن السيبراني–هيئة الإعلام- قسم الدراسات والاتصال والعلاقات العامة، الأردن- 2021

4- الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجاً. د. وفاء لطفي .مصر –جامعة 6أكتوبر - 2022

5- أنماط "الحرب السيبرانية" وتداعياتها علي الأمن العالمي. د. عادل عبد الصادق، المجلة السياسية الدولية- مصر – 2017.

6- الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، د. بن مرزوق عنترة– أستاذ محاضر في كلية الحقوق والعلوم السياسية بجامعة محمد بو ضياف–المسيلة-الجزائر 2021

7- مكتبة نور- كتاب البرمجيات الخبيثة .دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس واجراءات الوقاية منها - جميل حسن طويلة-26يوليو- 2015

8- الفريق الوطني للاستجابة لحوادث الأمن السيبراني(JoCERT) . الأردن، https://jocert.ncsc.jo/Default/Ar.2023

9 – جامعة الملك سعود . المملكة العربية السعودية . https://risk.ksu.edu.sa/ar/node/1480

10 - Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use .Bhargav-2018- Pingle; AakifMairaj; Ahmad Y. Javaid International Conference on Electro/Information Technology (EIT)

11- مؤسسة بصمة أمان للأمن السيبراني – المملكة العربية السعودية - https://www.secprint.sa/ddos-attacks/

/https://cypfer.com -12

Richard K. Betts, Conflict after the Cold War: Arguments on Causes of -13 War and Peace, 2nd ed. (New York: Longman, 2002): 548-557

Martin C. Libicki, Conquest in Cyberspace: National Security and -14 Information Warfare (New York: Cambridge University Press, 2007): 1-14

15- منشورات ITU الرقم القياسي العالمي للأمن السيبراني 2020

Global Cybersecurity Index 2024 5th EditionITUPublications -16 International Telecommunication Union Development Sector

(Secure Sockets Layer) SSL.com -17

/https://thehackernews.com -18

/https://asharq.com/technology/94302 -19

PEAKLIGHT Dropper: Hackers Target Windows With Downloads -20 by Wajahat Raja September 2, 2024 - TuxCare expert team

21- استراتيجية الأمن السيبراني للجمهورية العربية السورية – وزارة الاتصالات والتقانة

22- الوعي الاجتماعي بالأمن السيبراني لدى الطلبة (دراسة ميدانية على طلبة الجامعات طلبة كلية الامام الكاظم انموذجاً) ، أ.م.د.هديل تومان محمد البعاج/ كلية الامام الكاظم (ع)قسم الاعلام-2023

23- توفر الوعي بالأمن السيبراني لدى طلاب وطالبات جامعات السعودية من وجهة نظرهم، نورة بنت ناصر القحطاني، جمعية الاجتماعين، الشارقة، 2019.

24- استراتيجيات تعزيز الأمن السيبراني في المؤسسات الصناعية ضمن اطار التحول الرقمي – فلاح بن شهاب بن فلاح الظفيري، المجلة العالمية للعلوم الشرعية والقانونية – الإصدار السابع والأربعون، 2024