مدار للدراسات الاتصالية الرقمية | المجلد02/ العـدد:02 / نوفمبر (2022)، ص ص 01– 16

مدخل مفاهيمي حول الأمن السيبراني

Conceptual introduction to cyber security

أ.حميدي حياة [1*]، أ.طايلب نسيمة [2]

[1]جامعة الجزائر3، hayethamidi31@gmail.com

[2]جامعة شلف ، n.taileb@univ-chlef.dz

تاريخ الاستلام: اليوم 2022/03/09 تاريخ القبول: اليوم 2022/04/02 تاريخ النشر: اليوم 2022/11/01

ملخص:

نحاول ضمن هذه الورقة البحثية إثارة موضوع حساس، يشغل العام والخاص منا، من خلال التطرق إلى مفهوم الأمن السيبراني من حيث الدلالة والنشأة كمدخل لتشخيص الجرائم السيبرانية السائدة، ورفع أي لبس مفاهيمي للمصطلح، مع تحديد التداخلات المفاهيمية والإصلاحية الممكنة في حدود الاختصاص ومجال البحث.

وتندرج هذه الدراسة ضمن المساعي الوطنية والدولية لمعالجة قضايا الأمن الرقمي في مختلف المناسبات والمحافل (رسمية أو غير رسمية، وطنية أو دولية...)، على كافة المستويات المعنية (الأجهزة الأمنية، الجامعات، مخابر ومراكز البحث...) وضمن مختلف الأصعدة (الشخصية، المجتمعية والدولية...) تحت مسمى الجرائم المعولمة أو الجرائم العابرة للقوميات والحدود.

الكلمات المفتاحية: الأمن السيبراني، الجرائم السيبرانية، الفضاء الرقمي، تكنولوجيا الاعلام والاتصال، الأنظمة الحاسوبية.

*. حميدي حياة، المؤلف المرسل

Abstract:
the unlimited digital openness to the virtual environment has contributed to the exacerbation of digital crime and the multiplication of the number of its victims.Therefore, this study raises the issue of cybersecurity by addressing its concepts and the determinants of its emergence and development as an approach for diagnosing prevalent cyber crimes, and removing any conceptual confusion regarding them. This is in addition to trying to control the possible conceptual and terminological overlaps within the limits of the specialization and the field of research.
This study falls within the national and international endeavors to address digital security issues at all possible levels (security agencies, universities, laboratories and research centers...) and within various levels (personal, societal and international...) under the name of globalized crimes or transnational and border crimes.
Keywords:cyber security, cyber crimes, digital space, information and communication technology, computer systems

1. مقدمة:

نعيش اليوم في خضم مجتمع المعرفة والمعلومات، مجتمع الويب والاتصال الشبكي، أين أصبح التدفق المعلوماتي أسرع من أي تدفق آخر عرفته البشرية، فصارت مستحدثات هذه المرحلة تفوق بأشواط كبيرة المراحل الانسانية السابقة جودة وسرعة وسعة وثراء، وهو مانقل العالم من التقارب إلى التلاحم الجغرافي، لنتجاوز بذلك نبوة القرية الكونية لـ «**مارشالماكلوهان**»؛ هذا التدفق المعلوماتي ساهم في غزارة ووفرة معلوماتية غير مسبوقة أفضت إلى ظاهرة الانفجار المعلوماتي بما له وعليه من ايجابيات وسلبيات على المجتمع الدولي، كما تسبب من جهة أخرى في مشاكل أمنية

كثيرة متفاوتة الخطورة والضرر على الأفراد والدول، استدعت في الكثير من الحالات التدخل لحماية البيانات والمعلومات الشخصية والمشتركة خاصة ما تعلق منها بالسيادة الوطنية والأمن القومي، وهو ما يطلق عليه تسمية الأمن السيبراني.

فالدور الرئيسي للمعلومات في المجتمعات المعاصرة جعلها محل استهداف وتهديد يستدعي تأمينها وحمايتها من كافة الجرائم التي تواجهها، خاصة في ظل زيادة الاعتمادية على المعلومة كمصدر للثروة من جهة، وتزايد ارتباطية العالم ومؤسساته ببعضها لدرجة أضحى أمن مؤسسة معينة يهدد أمن مؤسسات أخرى نظرا لتشبيك الارتباط المعلوماتي بينهما.

وعلى هذا الاساس من الأهمية، وقع اختيارنا على موضوع الأمن السيبراني كنواة لورقتنا البحثية التي نحاولها من خلالها التعرض لمداخله المفاهيمية، من حيث النشأة، الدلالة والتطور، عناصره التركيبية، أهدافه وأهم التحديات التي تعرض إحلال الأمن السيبراني. من خلال طرح الاشكالية التالية:

ما هي المداخل المفاهمية الممكنة لفهم الأمن السيبراني وكافة القضايا الرقمية المتصلة به؟

تحقيقا لإشكالية الدراسة وموضوعها، تم طرح العديد من التساؤلات الفرعية، جاءت كالتالي:

- **ما المقصود بالأمن السيبراني؟**
- **ما هي المصطلحات المتصلة بالحروب السيبرانية ومختلف التهديدات الأمنية المستحدثة؟**

- **إلى أي مدى تشكل الحروب السيبرانية تهديدا فرديا وجماعيا على المجتمعات والدول؟**
- **كيف يمكن إحلال الأمن السيبراني في المجتمعات الرقمية المعاصرة؟**
- **ما هي أهم التحديات التي تواجه مساعي إقرار الأمن السيبراني؟**

للإجابة على إشكالية الدراسة وتساؤلاتها، اعتمدنا على المنهج الوصفي الذي يعد من المناهج البحثية الأكثر شيوعا واستخدامافي فهم الظواهر الراهنة من خلال تحليلها وتفسيرها العلمي المنظم بناء على وصفها كما هي عليه في الواقع، عن طريق الاحاطة بها واخضاعها للدراسة الدقيقة والتعبير عنها بشكل كيفيأو كمي، إذ يقتضي التعبير الكيفي وصف الظاهرة وتوضيح خصائصها، أما التعبير الكمي فيعطي وصفا إحصائيا للظاهرة بحصر حجمها وارتباطها بالظواهر الاخرى . (درويش، 2018، صفحة 118)وعليه، سنعمل في دراستنا على الاحاطة الكيفية بالموضوع، والتعريف بمختلف العناصر النظرية المتصلة بالتأصيل المفاهيمي للأمن السيبراني والمفاهيم المتصلة به،ابتغاء ازالة الغموض على أهم عناصره.

2. مفهوم الأمن السيبراني:

يعرف الأمن السيبراني حسب الهيئة الوطنية للأمن السيبراني (الهيئة الوطنية للأمن السيبراني، 2022)بأنه"تأمين كل الفضاء السيبراني الموجود والمترابط شبكيا من البنية التحتية لتقنية المعلومات، التي تشمل الانترنت وشبكات الاتصالات، وأنظمة الحاسب الآلي والأجهزة المتصلة بالانترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها"، كما أنه يعني(هيئة الاتصالات وتقنية المعلومات، 2020) بأنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة (عتاد)

وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي".

أما (المعهد الوطني للمعايير والتكنولوجيا ، بلا تاريخ، صفحة 2022)، فعرفه بأنه "حماية أنظمة الحاسب وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية والاتصالات الإلكترونية، بما في ذلك المعلومات الواردة فيها؛ واستعادتها لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك"، في حين أكد "إدوارد أموروسو"(دليل هارفارد بزنس ريفيو ، بلا تاريخ) بأن الأمن السيبراني يضم "مجموع الوسائل التي من شأنها الحد من اخطر الهجومات على البرمجيات أو أجهزة الحاسوب أو الشبكات"، فهو يبدأ بـ"الاحساس الفعلي والتخيلي بعدم وجود و/أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمع المعلوماتي(خاصة الحساسة منها) في جوانبها العسكرية، والاجتماعية، والثقافية، والاقتصادية...إلخ، المختلفة أيا كان مصدرها داخلي، أو خارجي، وتستدعي التأهب و/أو الفعل الاجتماعي و/أو التأهب والفعل الرسمي لمواجهتها". (البداينة، 2006، صفحة 23)

مما سبق يتضح أن الأمن السيبراني، تعلق في الأساس بحماية وتأمين مختلف الممارسات السيبرانية من مختلف التهديدات والمخاطر الممكنة والمحتملة والتي تمس فضاء صناعة وتداول المحتوى الرقمي بما يضمه هذا الفضاء الرحب من اليات ووسائل فاعلة ومتفاعلة في عملية نقل وحفظ وتخزين ومعالجة المعلومات والبيانات الرقمية، وتقع الأنظمة الحاسوبية وبرامج المعالجة ضمن أهم الحلقات المتصلة بتأمين المعلومة الرقمية. ويتعلق الامن السيبراني بالحفاظ على حقوق وواجبات الاستخدام الرقمي

للمعلومة إذ يحفظها لأصحابها مع منع ومحاربة أي استخدام غير مصرح، غير مشروع، غير قانوني

وعليه، فالأمن السيبراني عملية دفاعية وقائية تستهدف الاحاطة الأمنية التامة والشاملة للمعلومات والبيانات من كل استخدام غير مرغوب بما يقتضيه ذلك من صد للهجمات والجرائم الإلكترونية.

3. التداخلات المفاهيمية للأمن السيبراني:

- **الأمن السيبراني والفضاء السيبراني:**

أضحت عبارة الفضاء السيبراني مألوفة ومتداولة على ألسن الكثيرين فباتت تستخدم لوقف البيئة الإفتراضية للأنترنت وبقية وسائط الاتصال الرقمية التي ترتكز عليها المجتمعات المعلوماتية، إذ يعرَّف بأنه مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الانترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة"، غير أنه عمليا يتجاوز بعناصره الحدود التي تمتد عليها شبكة الأنترنت العملاقة، وبقية العوالم الإفتراضية المستحدثة، ليشمل كافة المستويات والأشكال والأنشطة الانسانية الاتصالية، باعتبار المجتمع الرقمي المعاصر ممتد عن العالم الواقعي ومكمل له ووثيق الصلة به. (البداينة، 2006، صفحة 49)فالأمن السيبراني انما هو تأمين وحماية لهذا الفضاء الافتراضي الذي ضمن سيولة معلوماتية رقمية تسري فيها المحتويات بمختلف أوعيتها ضمن فضاء غير محدود الاطر ولا مقيد الضوابط.

- **الأمن السيبراني وأمن المعلومات:**

يعرف أمن المعلومات بانه" حماية المعلومات من المخاطر التي تهددها من خلال ثلاث عناصر تشمل سرية المعلومة(confidentiality) وذلك من خلال ضمان الخصوصية، وسلامة البيانات(integrity)من خلال تكامُليّة وسلامة المحتوى، وأخيراً توافر المعلومة (Availability)من خلال إتاحة الوصول للمعلومات ويرمز لهذه العناصر الثلاث بـ CIA،ويتم ذلك من خلال وسائل وأدوات وإجراءات من أجل ضمان حمايتها من المخاطر سواءً كانت تهديدات داخلية أو خارجية"، ففي الوضع المثالي يجب دائما الحفاظ على سرية وتوفر وسلامة المعلومات لضمان تأمين أكبر لها، لذا فالملاحظ أن أمن المعلومات يهدف إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل.كما يستعين الأمن السيبراني بأمن المعلومات بكل الوسائل الضرورية لاكتشاف وتوثيق وصد كل التهديدات التي قد تعتري المعلومات والبيانات كما هو الحال في أنظمة تأمين الحماية للبنوك والمؤسسات المصرفية. (مجتمع تكنولوجيا المعلومات ، 2019)

- **الأمن السيبراني والأمن الالكتروني:**

يعبر مصطلح الأمن الإلكتروني عن "مجموعة الاجراءات الوقائية المتخذة لحماية المعلومات من السرقة أو الضياع أو التلف، ووضعها في شكل إمن لحمايتها من أي اعتداء عليها"، فهو يهدف لتوفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

- **من الناحية التقنية:** هو مجمل الوسائل والأدوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

- **من الناحية القانونية:** هو ما يقع محل دراسة وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.

4. مكونات الأمن السيبراني وعناصره التركيبية:

يشترط لتحقيق الأمن السيبراني وجود ثلاثة مركبات أساسية وهي:

- **الأدوات التقنية المستخدمةTechnology:**

تسمى أيضا بالبنية التحية لأنظمة المعلومات ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة

- **الإجراءات Processes:**

يندرج فيها كل الاجراءات التقنية والمادية والقانونية لتوفير هذه الحماية والأمن.

- **العامل البشري من مبرمجين ومستخدمين People:**

يضم كل الكفاءات والكوادر المكونة والمختصة في مجال الاعلام الآلي والذكاء الصناعي والتقني والالكتروني، من مهندسين وتقنيين سامين...الخ

5. أهداف الأمن السيبراني:

- يهدف الأمن السيبراني أولا وأخيرا إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل، وإلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين.

- تحسين مستوى حماية المعلومات وضمان استمرارية تدفقها وتشغيلها.
- ضمان انسيابية امنة للمعلومات وانتقال مشروع، مصرح ومرخص للملفات والبيانات.
- استرداد البيانات المسربة في أسرع وقت في حالة حدوث خرق للأنظمة الأمنية السيبرانية.

6. أهمية الأمن السيبراني:

من خلال أهداف الأمن السيبراني يظهر جليا الأهمية الأمنية لحماية المعلومات ومصادرها والأنظمة المرتبطة بحفظها وصيانتها واسترجاعها، وهذا ما نلمسه في العناصر التالية:

- **السلامة:** أي سلامة البيانات والمعلومات وحمايتها من أي هجوم أو خرق أو قرصنة.
- **السرية:** تكون كل المعطيات والبيانات والمعلومات في مأمن وغير مرخص أو مسموح لأي كان من الولوج إليها.
- **والجاهزية:** طالما أنها آمنة ومحمية فهي متاحة وجاهزة للاستعمال حسب الطلب والاتاحة.

فأهمية الامن السيبراني تكمن في العديد من الفوائد والميزات أهمها: (مجتمع تكنولوجيا المعلومات ، 2019)

- التقليل من مخاطر التهديدات الأمنية والاختراقات المحتملة للبيانات إلى جانب الحفاظ على سرية المعلومات.

- احلال الحماية الأمنية اللازمة للملفات الشخصية والحساسة لمنع الوصول غير المصرح إليها.
- ضمان استمرارية عمل المؤسسات المؤمنة وتجنب تعطيل مصالحها المتصلة بالاستخدام السيبراني لشبكة الانترنت، مع تقليل وقت التوقف عن الخدمات الرقمية خاصة الحساسة منها.

7. أنواع تهديدات الأمن السيبراني:

من الصعوبة حصر التهديدات الأمنية السيبرانية، فهي متنوعة ومتزايدة بأشكال رهيبة ويمكن تقسيمها إلى أربع فئات رئيسية، هي: (صبري و طارق، 2020، صفحة 105)

- التهديدات الأمنية التي تمس الشبكة الحاسوبية.
- التهديدات الأمنية التي تستهدف إختراق الحواسيب لتدمير البرامج والبيانات المتاحة به.
- التهديدات الأمنية التي تستخدم الحواسيب.
- التهديدات الأمنية التي تتممن خلال الاستغلال غير المرخص للبيانات المخزنة في الحواسيب.

ومن أكثر الجرائم التي تهدد الأمن السيبراني تتطلب حمايته من خلال برامج واليات مختصة بذلك، نجد:

- **تصيد المعلومات:**

يقصد به عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة. والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول. وهو أكثر أنواع الهجمات الإلكترونية شيوعًا. يمكنك المساعدة في حماية نفسك من خلال التثقيف أو استخدام الحلول التقنية التي تعمل على تصفية رسائل البريد الإلكتروني الضارة.

- **برامج الفدية ومرتزقة الأنترنت:** (صبري و طارق، 2020، الصفحات 109-110)

تعد برامج الفدية من البرامج الضارة التي يتم استخدامهاللوصول غير المصرح به إلى جهاز الكمبيوتر ومن ثم ابتزاز المال عن طريق منع الوصول إلى الملفات أو نظام الكمبيوتر حتى يتم تسديد الفدية، دون أن يضمن دفع الفدية استعادة النظام أو الملفات. ويعد مرتزقة الأنترنت أحد المجرمين الذين يتمرسون عملية الابتزاز والاسترزاق الإلكتروني تحقيقا لمأرب عدة من ضمنها "السادية الإلكترونية" التي يعمل ممارسها على إلحاق الأذى النفسي والمعنوي بالضحية والتلذذ بالجرم الإلكتروني.

- **الهندسة الاجتماعية:**

هي أسلوب يستخدمه القراصنة الرقميون في انتحال شخصية أفراد مهمين بهدف استدراج ضحاياهم إلى الكشف عن معلومات حساسة هم في حاجة لها لغرض أو لآخر،للقيام بذلك يتم طلب الحصول على دفع نقدي أو الوصول إلى البيانات السرية للضحية، وهناك العديد من الأدوات المساعدة على قرصنة الحواسب والدخول غير المرخص إلى مزودي الخدمة وسرقة أرقام بطاقات الائتمان المستخدمة، وكلمات المرور، ومن ثم سرقة معلومات مستخدمي هذه الشبكة. (البداينة، 2006، صفحة 292)

ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة سابقًا لزيادة فرص استدراج الضحايا، من خلال طلب النقر على الروابط أو تنزيل البرامج الضارة أو ترصد الوثوق بمصدر ضار.

8. تحديات الأمن السيبراني:

هناك عدة صعوبات وعراقيل تواجه الأمن السيبراني، وقد تكون على عدة مستويات وأصعدة، منها ما هو تقني ومادي ومنها ما هو بشري وذهني، ومنها ما هو داخلي أو خارجي...

- **عراقيل ذهنية أو بشرية:**

يساهم العامل البشري في عدة عراقيل ذلك أن المستخدمين أو الأفراد لا يراعون عند تسجيل المعلومات والبيانات طرق الحماية اللازمة والجيدة، مثل إدخال بعض البيانات بحماية محدودة، أو مشاركة المعلومات دون آليات حماية، ومحاولة خرق أمن الكتروني بإدخال رموز أو مفاتيح غير موجودة، وأشكال أخرى قد تكوّن ركنا من أركان الجريمة المعلوماتية، وتوقع عليه مسؤولية جنائية.

- **عراقيل على مستوى السلطات:**

تعجز الحكومات عن تحمل مسؤولية حماية الأفراد والمؤسسات من تهديدات تمس الأمن الرقمي والهجمات الرقمية، مع وجود فجوة كبيرة بين تقييمات التهديدات السيبرانية وتكاليفها ومجالات مسؤوليتها.

- **عر اقيل تقنية:**

تشكل التهديدات السيبرانية تحدياً مستعصيا، فهي بطبيعتها سريعة التغير، غير محدودة وغير متماثلة، ولذلك أصبح التنبؤ بها وإدارتها في غاية الصعوبة، كما أن هناك قدر قليل جداً من البيانات الإلكترونية المتاحة على نطاق واسع، ما يصعب عملية التقييم الموضوعي للتأثير المحتمل للحوادث.

- **عر اقيل في المنظومة التشريعية:**

ترتبط المعيقات التشريعية بنقصالتأطيرالقانوني الخاصة بالأمن السيبراني وسياسته وممارساته على نحو كامل، ذلك ان البيئة الالكترونية تتنامى بوتيرة أسرع وبشكل مستمر على وتيرة المشرع، وهو مايستوجب جهود واجتهادات فقهية لتكييف كل واقعة مرتبطة بالأمن السيبراني.

فتحقيق الأمن السيبراني يتطلب تجاوز العديد من التحديات من خلال تنسيق الجهود في محتلف النظم المعلوماتية الخاصة بها، وهي تشمل:(مجتمع تكنولوجيا المعلومات ، 2019)

أمن الشبكة، أمن الكومبيوتر، أمن البيانات، أمن شبكات الاتصال الهاتفي، أمن التطبيقات، أمن الأنظمة السحابية، أمن بنوك المعلومات وقواعدها التي تتشكل عموما من البنى التحتية المشكلة لهيكلة المجتمعات المعلوماتية، بالاضافة إلى التحدي الأكثر صعوبة وهو التجاوز المستمر للتهديدات المتنامية، فنفس التكنولوجيا المستعملة في الاختراق تستعمل في التأمين من الاختراق والتهديد الأمني، لذا وجبت المسايرة المستمرة

لتكنولوجيات تأمين المعلومات وتخزينها ومعالجتها. بالاضافة إلى ضرورة وضع خطط مسبقة للتصدي والتعافي من الهجمات والتهديدات الأمنية المحتملة.

9. خاتمة

بناء على ما سبق ذكره عن التأصيل النظري لمفهوم الأمن السيبراني ومختلف المصطلحات المتصلة والتي تشكل في مجملها، علاقة المعلومات والبيانات بمالكها وصانع ومستخدمها المشروع، فقد بدى جليا أهمية الوسائل والتطبيقات الرقمية في تحصين المعلومات والبيانات بنفس وسائل واليات الاختراق. لذلك توجب على المستخدم أن يكون ايجابيا في الاستخدام من خلال اكتساب ثقافة رقمية تسمح له بالإحاطة بواجبات وحقوق الاستخدام وعدم الوقوع ضحية لضعف أو انعدام الأمن السيبراني في وسائلهم المستخدمة.

فالثقافة الرقمية هي السلاح السابق لمختلف التهديدات السيبرانية، يليها شرط الإلمام بأبجديات الرقمنة وحدود الاستخدام العقلاني والمشروع، ومن ثم الاستعانة ببرامج الحماية التي تسمح بحد معقول من الحصانة الرقمية للملفات والبيانات الشخصية للأفراد والمؤسسات. وكلما زادت أهمية هذه الملفات والمعلومات كلما زادت الحاجة إلى تأمين أكبر وأعلى فعالية وقوة. لأن أغلب ضحايا التهديدات السيبرانية عادة ما يكونون من فئة الاشخاص المعلومين ذوي الصلة بالمجرم الالكتروني، أو ذوي النفوذ المالي والسياسي ابتغاء تحقيق أهداف الإبتزاز والجرم الإلكتروني عليهم.

وتبقى أقوى أنظمة الأمن السيبراني مهددة بالاختراق، بالنظر إلى الثغرات الأمنية الممكنة، لذا تبقى الحيطة والحصانة الرقمية، والوعي الرقمي أكثر الاساليب ردا لأغلب التهديدات الرقمية وأكثرها شيوعا.

10. التوصيات:

- أهمية الوسائل والتطبيقات الرقمية في تحصين المعلومات والبيانات بنفس وسائل واليات الاختراق.
- على المستخدم أن يكون ايجابيا في الاستخدام من خلال اكتساب ثقافة رقمية تسمح له بالإحاطة بواجبات وحقوق الاستخدام وعدم الوقوع ضحية لضعف أو انعدام الأمن السيبراني في وسائلهم المستخدمة.
- الإلمام بأبجديات الرقمنة وحدود الاستخدام العقلاني والمشروع.
- الاستعانة ببرامج الحماية التي تسمح بحد معقول من الحصانة الرقمية للملفات والبيانات الشخصية للأفراد والمؤسسات.

1. قائمة المراجع

أشرف صبري، و محمود طارق. (2020). جرائم العالم الإفتراضي. الدار الأكاديمية للعلوم .

المعهد الوطني للمعايير والتكنولوجيا . (بلا تاريخ). تم الاسترداد من https://aws.amazon.com/ar/compliance/nist/

الهيئة الوطنية للأمن السيبراني. (2022). تم الاسترداد من https://nca.gov.sa/news?item=272

دليل هارفارد بزنس ريفيو . (بلا تاريخ). تم الاسترداد من https://hbrarabic.com/%D8%A7%D9%84%D9%85%D9%81%D

8%A7%D9%87%D9%8A%D9%85-%D8%A7%D9%84%D8%A5
%D8%AF%D8%A7%D8%B1%D9%8A%D8%A9/%D8%A7%D9%
84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9
/%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A

ذياب البداينة. (2006). الأمن وحرب المعلومات (الإصدار 2). الأردن: دار الشروق للنشر والتوزيع.

مجتمع تكنولوجيا المعلومات . (2019). تم الاسترداد من https://itcomunity.com/post/%D9%85%D8%A7-%D9%87%D9%
88-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D
8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%9F-
%D8%AA%D8%B9%D8%B1%D9%8A%D9%81%D9%87-%D9%
88-%D8%B9%D9%86%D8%A7%D8%B5%D8%B1%D9%87-%D
9%88-%D9%85%D8%AC%D8%A7%D9%84%D8%A7%D

محمود أحمد درويش. (2018). مناهج البحث في العلوم الإنسانية. مصر : مؤسسة الأمة العربية .

هيئة الاتصالات وتقنية المعلومات. (2020). تم الاسترداد من https://www.cst.gov.sa/ar/mediacenter/pressreleases/Pages/202
00813.aspx