مجلة الشرق الأوسط للنشر العلمي
المجلد (٧) العدد (٣)
الإصدار الثالث العشرون
٢٠٢٤ (١٤-١)

العلوم التربوية والنفسية وعلاقتها بتحقيق الأمن السيبراني

د. معتصم تركي الضالعين
دكتوراة في العلوم الاجتماعية، كلية الدفاع المدني

نشر إلكترونياً بتاريخ: ٥ أغسطس ٢٠٢٤م

*** المقدمة**

تعد قضية أمن المعلومات وحمايتها من أهم القضايا في عصر الثورة الصناعية الرابعة – يعتمد نجاح أي منظمة إلى حد كبير على المعلومات التي تمتلكها، ولكن العديد من المعلومات والأنظمة والبنية التحتية المتصلة بالشبكة تكون في بعض الأحيان عرضة للخطر الهجمات لأنها تواجه أنواعًا مختلفة من الانتهاكات. كما تتعرض للنشاط الإجرامي (القرصنة) الذي يعطل خدماتها ويدمر ممتلكاتها، من ناحية أخرى، تختلف هجمات القرصنة، ومن وقت لآخر، تم استخدام أدوات وآليات تسلل مبتكرة ومتقدمة؛ وهذا يؤكد أهمية الأمن السيبراني في الحفاظ على سلامة الوطن والمواطنين.

أدت نهاية الحرب الباردة إلى العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والمعروفة باسم التهديدات العابرة للحدود التي لا تعترف بالحدود أو السيادة الوطنية أو فكرة الدول القومية، والتي تؤدي إلى الأمن. والتغيرات الاستراتيجية في مجال البحث ومستوى الممارسة السياسية.

في هذا السياق، تستهدف رؤية الأردن 2030 التنمية الشاملة للبلاد، والأمن، والاقتصاد، ورفاهية مواطنيها والحياة الكريمة. بطبيعة الحال، يتمثل أحد أهدافها في التحول إلى العالم الرقمي وتطوير البنية التحتية الرقمية؛ وهذا يعكس التقدم العالمي السريع في الخدمات الرقمية والشبكات العالمية المتجددة وأنظمة تكنولوجيا المعلومات وأنظمة التكنولوجيا التشغيلية، بما يتوافق مع قوة معالجة الكمبيوتر وتخزين البيانات الهائل وقدرات الاتصال في النمو والاستعداد للتغييرات في بيانات الذكاء الاصطناعي والثورة الصناعية الرابعة. (أبو زيد، ٢٠١٩)

الملخص

السؤال الأكثر أهمية للإجابة هو هل يستطيع علم النفس تحسين الأمن السيبراني؟ في الواقع، يمكن لمنصات الوسائط الاجتماعية وجميع المنصات عبر الإنترنت بشكل عام اتخاذ خطوات لزيادة الوعي، مثل تحديد السياقات الاجتماعية التي قد يشارك فيها الأشخاص المعلومات الخاصة، والبحث عن أنماط النشاط الضار، وتعزيز التعاون مع المشرعين، وزيادة الوعي العام وفهم تأثير الجريمة على الويب. على سبيل المثال، من المرجح أن يكشف الأفراد عن معلومات شخصية وحساسة في المحادثات غير الرسمية والشبكات الاجتماعية، لذلك يجب دائمًا تذكير المستخدمين قبل مشاركة هذه البيانات.

تعد القرصنة والخروقات والخداع ورسائل البريد الإلكتروني الاحتيالية والسرقة من أهم مخاوف الأمن السيبراني. من هذا الصراع الرقمي، يجب أن تظهر ثقافة الأمن السيبراني في التعليم.

Abstract

The most important question to answer is can psychology improve cybersecurity? In fact, social media platforms and all online platforms in general can take steps to raise awareness, such as identifying social contexts in which people may share private information, looking for patterns of malicious activity, enhancing cooperation with lawmakers, and raising public awareness and understanding of the impact of crime on the web. For example, individuals are more likely to disclose personal and sensitive information in casual conversations and social networks, so users should always be reminded before sharing this data.

Hacking, breaches, phishing, phishing emails and theft are some of the top cybersecurity concerns. The culture of cyber security appears in education.

*** هدف البحث**

تهدف هذه الورقة إلى إلقاء الضوء على مشاكل التحول الرقمي التي أصبحت حقيقة واقعة، والتي تتوافق إلى حد كبير مع الحركة التحويلية التي يشهدها العالم والمعرفة والمعلومات والثورة الرقمية والتداخل الهائل في هذا التحول. يمثل جميع جوانب ومستويات التفاعل سواء كانت سياسية أو اجتماعية أو اقتصادية أو تعليمية أو فكرية وأيديولوجية وغيرها، ومدى تأثير هذا التحول الرقمي على حياة الإنسان والتعليم، أي أن المجتمع يحقق له الأساس الفوري للاستعداد النوعي للأعضاء، وهو ضمان التكوين الصحيح للأفراد في مثل هذه المواقف وقيمهم التي تشكل معايير واضحة تحفز الوجود والتفاعل المؤسسي الإيجابي. تكشف هذه الورقة عن مشكلة التحول الرقمي وأثرها الخطير على الأمن التعليمي من مختلف الأبعاد، وتحاول وضع إطار للتفكير للتخلص من هذه المشكلة الخطيرة .

*** مشكلة البحث**

على الرغم من أن تقنية المعلومات قد حققت مزايا كبيرة، إلا أن هذه الثورة المعلوماتية المتصاعدة قد ترافقت أيضًا

مع بعض الآثار السلبية الخطيرة بسبب سوء الاستخدام. نطاق بلد معين، والذي يمثل عدداً من التحديات القانونية للوكالات المشاركة في مكافحة الجريمة.

في الآونة الأخيرة، أصبحت كلمة الأمن السيبراني شائعة، وقد سمع هذا المصطلح العديد من الخبراء في مجال أمن المعلومات، وظهرت العديد من الأسئلة، بما في ذلك، ما هو الأمن السيبراني، وما هو جزء أمن المعلومات في الأمن السيبراني، وما الفرق بينهم؟؟ على من ينطبق المصطلح وما التهديدات التي يحمي الأمن السيبراني منها؟ هل هي فقط للمؤسسات أم ضد المؤسسات والأفراد، وكيف نمنع حروب الجيل الرابع؟

*** الغرض من الدراسة**

التعرف على متطلبات نظام المعلومات الإدارية لتحقيق الأمن السيبراني وعلاقة الأمن السيبراني بالعلوم التربوية والنفسية .

*** أهمية البحث**

تكمن أهمية البحث في البحث نفسه، لأن البحث التربوي في مجال أمن شبكات المعلومات لا يزال محدوداً، والهجمات الإرهابية ما زالت مستمرة، وقد تزداد مع التطور التكنولوجي والثورات المعرفية .

*** مصطلح البحث**

*** الأمن السيبراني**

جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به ولحماية المعدات والبيانات.

*** الإطار النظري والبحوث السابقة**

بحث أجراه المعهد العربي للتخطيط (2016) مخاطر الهجوم السيبراني وأثره الاقتصادي: دراسة حالة لدول مجلس التعاون الخليجي تحاول هذه الدراسة إلقاء الضوء على أهمية المخاطر الإلكترونية وتأثيرها الاقتصادي وكيفية إدارتها، إعطاء النمذجة الدولية لأحداث العدوى، ثم تحليل وتقييم دول مجلس التعاون الخليجي. تتقدم دول مجلس التعاون الخليجي على بقية العالم في أنواع معينة من الهجمات الإلكترونية على النشاط الاقتصادي، على سبيل المثال، على الرغم من دول مجلس التعاون الخليجي هي استجابة للهجمات السيبرانية. تحسن الأداء، لكن الهجمات الإلكترونية في الدولة المتوسطية العالمية تكلف أكثر من الخسائر (البريد الإلكتروني العشوائي).

ومع ذلك، فإن الإرشادات العلمية بشأن الأمن السيبراني الصادرة عن الأمم المتحدة تظهر أن هناك العديد من الثغرات القانونية والتقنية والتنظيمية والتدريبية والتعاونية في هذه المجالات التي يجب سدها من خلال تحسين الأداء واستكمال ومراجعة الوضع الراهن. إن زيادة الإنفاق وحده لن يكون كافياً لدول مجلس التعاون الخليجي لمواجهة التهديدات وتحقيق الأمن السيبراني، بل يجب أيضاً تحسين الوعي والحوكمة والعمليات، حيث تتمتع المنطقة بواحد من أكثر معدلات تبني التكنولوجيا الحديثة تطوراً في العالم.

حاولت دراسة (El Hissi et al.، 2018) اقتراح إطار حوكمة للأمن السيبراني للجامعات الحكومية المغربية. وخلصت الدراسة إلى أن استخدام أنظمة الأمن السيبراني في المؤسسات الأكاديمية من شأنه أن يجلب العديد من الفوائد الإدارية والمالية والأكاديمية .

دراسة (العتيبي ،2017) حول دور الأمن السيبراني في تعزيز الأمن البشري: –

تحاول الأسئلة البحثية الإجابة على سؤال رئيسي واحد: –

١– ما هو دور الأمن السيبراني في تعزيز الأمن البشري؟

٢– تكون مجتمع الدراسة من العاملين في الأمن السيبراني ضمن مقياس أميليا السعودي، وتم اختيار عينة الدراسة (400 شخص) بشكل عشوائي. (أبو زيد ،٢٠١٩)

٣– التدابير الفنية لحماية الفضاء السيبراني للشركة متاحة على نطاق واسع، يقفل النظام تلقائيًا عندما لا يكون قيد الاستخدام لفترة زمنية محددة.

٤– التوافر الواسع للإجراءات التقنية لحماية الفضاء السيبراني للشركات.

٥– استخدام القياسات الحيوية (بصمات العين، بصمات الأصابع، بصمات الصوت) لتصاريح الدخول المصرح بها.

يقترح الباحث ضرورة اتباع نهج علمي وعملي لحماية الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة، ويوصي أيضًا بإجراء دراسة أكثر تعمقًا للروابط بين مجال الأمن السيبراني والأمن البشري.

دراسة (البكري، 2017) حول أمن المعلومات في مكتبات جامعة السودان إلى تحديد مخاطر عدم تأمين المعلومات في مكتبات الجامعة وكيفية تأمينها. استخدمت الدراسة الأساليب التاريخية، من خلال النظر في المؤلفات المنشورة وأدوات المراقبة في مكتبة جامعة السودان. (أبو زيد ،٢٠١٩)

*** الوكالة الوطنية للأمن السيبراني**

مع اندلاع ثورة المعلومات ودخول العصر الرقمي، خاصة في القرن الحادي والعشرين، والتأثيرات العديدة لظهور التهديدات والجرائم السيبرانية، أصبحت تشكل تحديًا كبيرًا للأمن الوطني والدولي، لذلك لدرجة أن العديد من الدراسات يعتبر الناس الفضاء السيبراني هو المجال الخامس للحرب بعد الأرض والبحر والجو. وينعكس مجال الأمن في هذه البيئة الرقمية بشكل أساسي في ظهور الأمن السيبراني كبعد عسكري. جدول أعمال في مجال البحث الأمني وتحظى باهتمام العديد من الباحثين في هذا المجال. (الشيتي ،٢٠١٩)

أبحاث الأمن السيبراني أحد التطورات التكنولوجية الحديثة والابتكارات التكنولوجية المتطورة التي تعايشت في جميع أنحاء العالم، وتشهد الدول المتقدمة تطورات ضخمة لا يمكننا تجاهلها في كل جانب. نتيجة لذلك، أصبحت هذه الدراسات الفنية في مجال الحوسبة الرقمية وجهة للعديد من العلماء المتميزين حول العالم، لكن التطور الرقمي الذي تشهده له جانب مظلم آخر، والذي قد يهدد تغلغل الدول الكبرى والشركات والأعمال والمؤسسات الاقتصادية، وربما هذا هو أحد أسباب أهمية دراسة الأمن السيبراني، والتي تسعى لحماية البيانات والشبكات والأنظمة الإلكترونية من الهجمات والاختراقات التي قد تؤدي إلى استقرارها واستقرارها. لذلك، من الضروري فهم طبيعة الأمن السيبراني وإجراء البحوث العلمية والمتعمقة حوله من مختلف جوانبه كمتغير جديد في العلاقات الدولية. (جبور، منى الأشقر ،2016(

دراسة.Rehman et al) ، 2015 (عن الحالة الحالية لأنظمة إدارة الأمن السيبراني في مؤسسات التعليم العالي

بالجامعة الباكستانية الحاجة إلى إدارة المخاطر الحالية وتطوير سياسات أمنية لمعالجتها.

*** الأمن السيبراني ومفاهيمه وأهميته وأهدافه**

*** مفهوم الأمن السيبراني**

*** معنى كلمة السيبراني**

(cyber) تشير كلمة cyber إلى كل ما يتعلق بشبكات الكمبيوتر الإلكترونية ، وتشير الإنترنت والفضاء الإلكتروني إلى الفضاء السيبراني ، والذي يشير إلى شبكات الكمبيوتر والإنترنت والتطبيقات المختلفة مثل WhatsAppو Facebook ومئات غيرها.)) ، وجميع الخدمات التي تنفذها (مثل تحويل الأموال عبر الإنترنت والمشتريات عبر الإنترنت وآلاف الخدمات الأخرى في جميع مجالات الحياة العالمية) .(الشيتي، ايناس ،ابراهيم ،٢٠١٩)

*** الأمن السيبراني**

الأمن السيبراني هو حماية الأشياء من خلال تكنولوجيا المعلومات, مثل الأجهزة والبرامج ، التي يشار إليها باسم تكنولوجيا المعلومات والاتصالات ، يشير أمان الشبكة إلى اتخاذ التدابير اللازمة لحماية الفضاء الإلكتروني من الهجمات الإلكترونية ، ومنع الوصول غير القانوني إلى المعلومات الإلكترونية ومنع تطورها غير القانوني والمنهجي من خلال مجموعة من الوسائل التقنية والتنظيمية والإدارية ، لذلك يهدف أثناء الصيانة إلى ضمان استمرارية الأنظمة والمعلومات المتوفرة فيها وحماية خصوصيتها وسريتها باتباع الإجراءات والتدابير اللازمة لحماية البيانات. (الشيتي- ايناس ابراهيم ،٢٠١٩)

*** الأمن السيبراني لغوياً**

يتكون الأمن السيبراني من كلمة "الأمن"، وهي نقيض الخوف وتعني الأمن والأمان. من أكثر المصطلحات استخدامًا في قواميس الأمن الدولي، كلمة "cyber" مشتقة من الكلمة اليونانية"kybernetes" ، وتعني الشخص الذي يوجه دفة السفينة. Norbert 1894-1964 (Wieners)للتعبير عن التحكم الآلي.

يحتوي مفهوم الأمن السيبراني على العديد من التعريفات، حيث يتم تعريفه على أنه "مجموعة التدابير المتخذة في مجال التراع ردًا على هجوم إلكتروني وعواقبه، بما في ذلك تنفيذ الإجراءات المضادة المطلوبة."

هذا ما قاله المؤلفان Neitaanmaki Pekka و Lehto Marttiفي كتابهما "تحليل الأمن السيبراني والتكنولوجيا والأتمتة"، فقد عرفا الأمن السيبراني بأنه: "محاولة للدفاع ضد هجمات القرصنة على الكمبيوتر وعواقبها. سلسلة من التدابير، بما في ذلك تنفيذ التدابير المضادة اللازمة ". (جبور، منى الأشقر ،2016)

ويعتقد عداءه (إدوارد أموروسو إدوارد) أنه "عن طريق الحد من مخاطر الهجوم على البرامج أو أجهزة الكمبيوتر أو الشبكات، بما في ذلك أدوات مكافحة القرصنة، واكتشاف الفيروسات وتوقيتها، وتوفير الاتصالات المشفرة."

في تقرير نشره الاتحاد الدولي للاتصالات حول اتجاهات إصلاح الاتصالات في 2011. (201) غرفة الأمن السيبراني بمثابة "مجموعة من المهام، مثل تجميع الأدوات والسياسات والإجراءات الأمنية، والمبادئ التوجيهية وطرق إدارة المخاطر، والتدريب، وأفضل الممارسات، والتقنيات التي

يمكن استخدامها لحماية البيئة السيبرانية والأصول التنظيمية والمستخدمين ". (الشيتي، ايناس ابراهيم ،٢٠١٩)

تقدم وزارة الدفاع الأمريكية تعريفًا دقيقًا لمصطلح الأمن السيبراني، معتبرةً إياه "جميع التدابير التنظيمية اللازمة لضمان حماية جميع المعلومات في الشكل المادي والإلكتروني من الجرائم بجميع أنواعها: الهجمات والتخريب والتجسس والحوادث"، بينما يرى الإعلان الأوروبي أن الأمن السيبراني هو قدرة أنظمة المعلومات على مقاومة محاولات التسلل ضد البيانات "

وتجدر الإشارة إلى أن أمن الشبكة أوسع من أمن المعلومات، لأن أمن الشبكة يركز على أمن كل ما هو موجود على الشبكة، ولا يوجد أمن معلومات، وأمن المعلومات لا يلتفت إلى ذلك، ويركز أمن المعلومات على الأشياء الورقية . (الشيتي، ايناس ابراهيم ،٢٠١٩)

*** أهم أهداف الأمن السيبراني**

١- تعزيز حماية أنظمة التكنولوجيا التشغيلية على جميع المستويات ومكونات أجهزتها وبرامجها والخدمات التي تقدمها والبيانات التي تحتويها.

٢- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الجهات الحكومية وكذلك هيئات القطاعين العام والخاص (جبور، منى الأشقر ،2016)

٣- توفير بيئة آمنة ومأمونة للمعاملات في مجتمع المعلومات.

٤- صمود البنية التحتية الحساسة للهجمات الإلكترونية.

٥- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية ضد المستخدمين.

٦- القضاء على نقاط الضعف في مختلف أنظمة الكمبيوتر والأجهزة المحمولة.

٧- سد الثغرات في أنظمة أمن المعلومات .

٨- مقاومة البرمجيات الخبيثة المصممة لإحداث أضرار جسيمة للمستخدمين. (أبو زيد ،٢٠١٩)

٩- الحد من أعمال التجسس والتخريب الإلكترونية على مستوى الحكومة والأفراد.

١٠- اتخاذ كافة الإجراءات اللازمة لحماية المواطنين والمستهلكين من المخاطر المحتملة في كافة مجالات استخدام الإنترنت.

١١- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة تحديات اختراق الأجهزة التقنية التي تتلف معلوماتهم الشخصية بغرض التخريب أو السرقة .

*** أهمية الأمن السيبراني**

في الشبكة المترابطة اليوم، يستفيد الجميع من خطة الدفاع السيبراني، وتكمن أهمية الأمن السيبراني فيما يلي:-

١- الحفاظ على المعلومات وسلامتها وتجانسها، من خلال منع الناس من العبث بها، وتدمير كميات كبيرة من البيانات واستعدادها عند الحاجة .

٢- حماية المعدات وعمليات التفتيش من التخريب كدرع وقائي للبيانات والمعلومات .

٣- استكشاف ومعالجة نقاط الضعف .

٤- استخدام أدوات مفتوحة المصدر وتطويرها لتنفيذ شبكة مبادئ الأمان.

٥- يوفر بيئة عمل آمنة للغاية عند العمل على الإنترنت.

*** أهمية الأمن السيبراني**

تعد أبحاث الأمن السيبراني من أهم المجالات التي تحتاج إلى خبراء مؤهلين لحماية أمن الشركات والمؤسسات والدول لعدد من الأسباب أبرزها:-

١- هناك حاجة مستمرة لخبراء في مجال الأمن السيبراني في سوق العمل

٢- هناك فوائد اقتصادية كبيرة يمكن اكتسابها من خلال العمل في مجال الأمن السيبراني.

٣- ستكون الخبرة في مجال الأمن السيبراني هدف كل شخص متميز منظمة.

٤- يمنح الطلاب امتيازات فريدة في الوظيفة أهم مسار وظيفي بعد تعلم الأمن السيبراني.

شهد هذا المجال طلبًا كبيرًا في مختلف المجالات، لذلك تظهر التقارير والإحصاءات العالمية أن الطلب على متخصصي الأمن السيبراني قد زاد بشكل كبير، حيث نما سوق الأمن السيبراني وتطور بشكل كبير في مختلف دول العالم، يقدر بنحو 3.5 مليار دولار في عام 2004.، مقارنة بـــ 75 مليار دولار في عام 2015، ومن المتوقع أن تصل إلى ما يقرب من 170 مليار دولار عالميًا في عام 2020، (https://ab7as.net) بعد دراسة الأمن السيبراني والحصول على درجة البكالوريوس ، من المتوقع أن يجد الخريجون العديد من الفرص الوظيفية المتميزة في مجموعة متنوعة من المجالات. تختلف المسارات الوظيفية لهذه الدراسة وتشمل: مهندس الدعم السحابي، وأخصائي دعم تكنولوجيا المعلومات، ومهندس الدعم الفني، ومطور البرامج والتطبيقات. مدير الشبكه. ضابط الطب الشرعي الرقمي. (جبور ،2016).

*** الأمن الإلكتروني**

هي مجموعة من الوسائل الفنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به وسوء الاستخدام واستعادة المعلومات الإلكترونية وأنظمة الاتصال والمعلومات التي تحتويها، مصممة لضمان توافر واستمرارية تشغيل أنظمة المعلومات، وكذلك لتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. الأمن السيبراني هو سلاح استراتيجي في أيدي الحكومات والأفراد، خاصة وأن الحرب الإلكترونية أصبحت جزءًا لا يتجزأ من الحرب الحديثة واستراتيجيات الهجوم بين الدول.

في عصر التكنولوجيا، يلعب أمن المعلومات الدور الأكبر في الدفاع ضد ومنع أي هجمات إلكترونية قد تتعرض لأنظمة الدولة المختلفة وحماية نظام التشغيل من أي محاولات للوصول غير المصرح به إلى أهداف غير مشروعة، وإليكم السبب وراء ذلك. الأمر الملكي بإنشاء الوكالة الوطنية للأمن السيبراني .

*** دورها**

نظرًا للأهمية المتزايدة للأمن السيبراني في الحياة الاجتماعية، تهدف الوكالة إلى تعزيز حماية الشبكات وأنظمة تكنولوجيا المعلومات وأنظمة التكنولوجيا التشغيلية ومكونات الأجهزة والبرامج الخاصة بها والخدمات التي تقدمها والبيانات التي تحتويها.

*** الأولويات**

وستعطي الهيئة الأولوية لاستقطاب الكوادر الحكومية المؤهلة والطموحة وتطويرها، وإقامة شراكات مع الجهات العامة والخاصة، وتحفيز الابتكار والاستثمار في الأمن السيبراني لتعزيز النهضة التكنولوجية التي تخدم مستقبل الاقتصاد الوطني للمملكة.

صدر الأمر الملكي بإنشاء جهاز خاص بحامي الحرمين الشريفين باسم الجهاز الوطني للأمن السيبراني، بالموافقة على تنظيمه، وتعيين الدكتور مساعد بن محمد العيبان عضواً في الهيئة العامة للأمن السيبراني. مجلس الوزراء معالي وزير الدولة رئيساً لمجلس الإدارة. (البكري، يوسف الشيخ ،٢٠١٧)

*** هاكر**

بشكل عام، الاختراق هو القدرة على الوصول بشكل غير قانوني إلى هدف معين بالطبع، من خلال ثغرة في نظام حماية الهدف، يستطيع المخترق الوصول عمدًا إلى جهاز شخص آخر، عن غير قصد أو حتى بدون علمه، وهي ميزة سيئة، بغض النظر عن الضرر الجسيم الذي قد يتسبب فيه، سواء كان ذلك أم لا. عندما يسحبون متعلقاتهم ووثائقهم وصورهم أو أجهزتهم الشخصية أو عقولهم. ما الفرق بين قرصنة الأجهزة الشخصية والقرصنة الآمنة للمنازل؟ عرياتم تعني اختراق وحقرته .

*** أسباب الاختراق ودوافعه**

هذه الظاهرة لا تنتشر فقط بسبب العبث، وإن كان العبث وقتل وقت الخمول من أبرز العوامل التي تسهم في تطورها وظهورها في عالم الوجود. يلخص المؤلفون الثلاثة للمراجع التي أستخدمها في هذه الدورة الدوافع الرئيسية للاختراق في ثلاث نقاط، والتي ألخصها هنا على النحو التالي:-

١- الدافع السياسي والعسكري: مما لا شك فيه أن تطور العلوم والتكنولوجيا أدى إلى الاعتماد شبه الكامل على أنظمة الكمبيوتر لمعظم الاحتياجات التقنية والمعلوماتية. كان الصراع على المعلومات والتجسس بين القوتين العظميين هو الأشد حدة منذ الحرب الباردة. مع ظهور مناطق نزاع جديدة في العالم والطبيعة المتغيرة للأنظمة والمعلومات الوطنية، أصبح الاعتماد على أجهزة الكمبيوتر يعتمد بشكل كامل على أجهزة الكمبيوتر، وأصبحت وسائل التسلل للمعلومات السياسية والعسكرية والاقتصادية أكثر أهمية. سؤال. (جبور، منى الأشقر ،2016)

٢- الدوافع التجارية: من المعروف أن الشركات التجارية الكبرى في حالة حرب مع بعضها البعض. تظهر الأبحاث الحديثة أن العديد من الشركات التجارية الكبيرة تواجه أكثر من خمسين محاولة لاقتحام شبكاتها كل يوم .

*** تعريف العلوم التربوية وعلم النفس السيبراني**

علم النفس السيبراني هو مجال يركز على دراسة العقل في سياق التفاعل بين الإنسان والحاسوب. مع حدوث جزء كبير من أنشطتنا اليومية عبر الإنترنت (مثل التفاعلات الاجتماعية، والتسوق، والخدمات المصرفية، والقراءة، وبث الفيديو والموسيقى، وما إلى ذلك)، فلا عجب أننا قلقون بشكل متزايد بشأن كيفية تأثير التكنولوجيا على أفكارنا وسلوكياتنا، وفي النهاية كيف نشكلها. كأفراد وكمجتمع! (البكري، يوسف الشيخ ،٢٠١٧)

على سبيل المثال، يمكن تطبيق علم النفس السيبراني على ألعاب المقامرة الافتراضية التي تقدمها الكازينوهات عبر الإنترنت لفهم ما يحفز اللاعبين على لعب هذه الألعاب ولتحديد أسباب إدمانهم، وربط نتائج هذه الدراسة بالبحث الذي أجري على الكازينوهات التقليدية قارن.

يأتي مصطلح "Cyber" من "علم التحكم الآلي"، وهو مجال دراسة أنظمة التحكم والاتصالات. علم النفس هو دراسة السلوك البشري والفكر. وفقًا لجون سولير، ظهر المصطلح في منتصف التسعينيات واستخدمه الباحثون السلوكيون عبر الإنترنت .

باختصار، يدرس علم النفس السيبراني تنمية الشخصية في وسائل الإعلام عبر الإنترنت، والعلاقات التي نطورها عبر الإنترنت، وإدمان التكنولوجيا والتسلط عبر الإنترنت.

*** لماذا علم النفس السيبراني مهم؟**

نظرًا لأن الخطوط الفاصلة بين الفضاء الإلكتروني والعالم الحقيقي غير واضحة، فمن الأهمية بمكان دراسة وفهم السلوك البشري فيما يتعلق بالتكنولوجيا. بالطبع، سيكون من السذاجة الاعتقاد بأن التكنولوجيا لن تؤثر على الجميع بطريقة ما!

يهتم علم النفس السيبراني بالإجابة على الأسئلة التالية:-

١- لماذا يتصرف الناس على الإنترنت بشكل مختلف عن الحياة الواقعية؟ (جبور، منى الأشقر ،2016)

٢- كيف تتطور علاقات الشبكة؟ هل يظهر الناس بشخصيات مختلفة في الفضاء السيبراني؟

٣- مع تزايد التداخل بين البشر والآلات، أصبح تطوير هذه المهنة أمرًا ضروريًا .

٤- أظهرت العديد من الدراسات أن التعرض المفرط لمحتوى الإنترنت يؤثر على الصحة العقلية لمستخدمي الإنترنت. (حجازي، عبد الفتاح بيومي (2007 م)

على سبيل المثال، قد يتم تقصير فترة انتباههم، وقد يصبحون مدمنين على التكنولوجيا أو تضللهم ظاهرة الأخبار المزيفة!

في النهاية، تهدف أبحاث علم النفس السيبراني إلى تمكيننا من جعل الإنترنت مكانًا أفضل وأكثر أمانًا.

*** ما علاقة علم النفس بالأمن السيبراني؟**

للوهلة الأولى، قد يبدو أن الأمن السيبراني يتعلق فقط بتكنولوجيا المعلومات، في حين أنه في الواقع يرتبط ارتباطًا وثيقًا بعلم النفس. لماذا ا؟ (جبور، منى الأشقر ،2016)

*** الجواب بسيط**

يمكن للنفسية البشرية أن تثبت أنها عامل تمكين حقيقي للجرائم الإلكترونية! في الواقع، أظهرت الأبحاث على مر السنين أن الخطأ البشري لا يزال يبدو أنه السبب الجذري للعديد من انتهاكات البيانات .

فيما يلي المجالات الرئيسية الثلاثة للبحث في مجال علم النفس السيبراني:-

١- هندسة اجتماعية .

٢- الخصوصية عبر الإنترنت .

٣- التنمر الإلكتروني .

يمكن التلاعب بالأشخاص بسهولة لتنفيذ إجراءات معينة تسهل الهجمات الإلكترونية. على سبيل المثال، التصيد هو هجوم مستهدف مصمم لخداع أفراد معينين للكشف عن معلومات سرية أو تنزيل مرفقات بريد إلكتروني ضارة أو النقر فوق روابط مشبوهة وإصابة أجهزة الضحايا ببرامج ضارة.

يعتمد هذا الهجوم، إلى جانب العديد من الهجمات الأخرى مثل التصيد الاحتيالي أو برامج الفدية، على الهندسة الاجتماعية وهو ممارسة شائعة لمجرمي الإنترنت. في الأساس، في مجال أمن تكنولوجيا المعلومات، تنجح هجمات الهندسة الاجتماعية بسبب التلاعب النفسي.

بغض النظر عن مدى قوة تدابير الأمن السيبراني الخاصة بك، فإن معلوماتك الشخصية أو بيانات الشركة السرية معرضة للخطر. إذا كنت لا تعرف أنه يتم التلاعب بك للقيام بشيء مثل التخلي عن بيانات اعتماد تسجيل الدخول أو التفاصيل المصرفية أو حتى تحويل الأموال، فيمكنك بسهولة الوقوع فريسة لمجرمي الإنترنت في الهندسة الاجتماعية.

يبدو أيضًا أن الخصوصية عبر الإنترنت موضوع ساخن في مجال علم النفس السيبراني. من خلال أبحاثهم، يحاول الخبراء العثور على إجابات لأسئلة معينة، مثل: – (البكري، يوسف الشيخ ،٢٠١٧)

١– كيف يؤثر العمر على سلوك الحفاظ على الخصوصية على وسائل التواصل الاجتماعي؟

٢– ما مدى قلق الناس بشأن حماية خصوصيتهم على الإنترنت؟

٣– ما هي طرق حماية الخصوصية التي يستخدمونها عبر الإنترنت؟

بدأ بحث التسلط عبر الإنترنت كرد فعل على الاستخدام المتكرر للتكنولوجيا من قبل المراهقين لتحديد ودراسة تأثير التنمر على الناس. (حجازي، عبد الفتاح بيومي ،2007 م)

يبدو أيضًا أن الخصوصية عبر الإنترنت موضوع ساخن في مجال علم النفس السيبراني. من خلال أبحاثهم، يحاول الخبراء العثور على إجابات لأسئلة معينة، مثل:– (حجازي، عبد الفتاح بيومي ،2007 م)

١– كيف يؤثر العمر على سلوك الحفاظ على الخصوصية على وسائل التواصل الاجتماعي؟

٢– ما مدى قلق الناس بشأن حماية خصوصيتهم على الإنترنت؟

٣– ما هي طرق حماية الخصوصية التي يستخدمونها عبر الإنترنت؟

بدأ بحث التسلط عبر الإنترنت كرد فعل على الاستخدام المتكرر للتكنولوجيا من قبل المراهقين لتحديد ودراسة تأثير التنمر على الناس.

*** ما هي ثقافة الأمن السيبراني؟**

قبل وصولCOVID-19 ، كانت معظم المدارس قلقة للغاية بشأن الأمن السيبراني. ومع ذلك، مع الوباء، زادت هجمات الأمن السيبراني المختلفة، مما تسبب في مشاكل للموظفين والطلاب وأولياء الأمور.

الحل الآن هو بناء ثقافة الأمن السيبراني على جميع مستويات التعليم.

*** ما هي بالضبط ثقافة الأمن السيبراني؟**

يعد هذا مصدر قلق جماعي للأمن السيبراني في جميع أنحاء المدرسة حيث يعمل الجميع معًا لتحديد ومنع ووقف الهجمات بجميع أنواعها. ستشمل هذه الثقافة أشياء بسيطة مثل استخدام كلمات مرور قوية وأشياء أعمق مثل معرفة علامات المتسلل.

نظرًا لأن المدارس بها الكثير من الأشخاص الذين يتعلمون ويعملون عن بُعد أو شخصيًا، يجب إنشاء ثقافة الأمن السيبراني. (حجازي، عبد الفتاح بيومي ،2007 م)

تشمل أفضل الممارسات التدريب والتعليم والإدارة واستخدام الأنظمة الصحيحة والحفاظ على محادثة مستمرة حول الأمن السيبراني.

بعبارة أخرى، الهدف من ثقافة الأمن السيبراني هو تطبيع هذه المواضيع والمجالات، وجعلها طبيعة ثانية للجميع في التعليم.

لتحقيق ذلك، يجب على كل مؤسسة تعليمية اتخاذ الخطوات الصحيحة للاندماج والتدريب. (جبور، منى الأشقر ،2016)

*** بناء ثقافة الأمن السيبراني**

لبناء ثقافة الأمن السيبراني في التعليم، فإن الخطوات التالية ضرورية. بعد ذلك سيتفهم كل فرد في المدرسة أهمية حماية المعلومات والبيانات في عالم الإنترنت.

١- إعادة التقييم

الخطوة الأولى هي التراجع خطوة إلى الوراء

تحتاج الإدارة وأي عوامل فنية إلى إلقاء نظرة على الصورة الكبيرة. اين المدرسة الان ما مدى ضعف بيانات المدرسة ومعلوماتها عن الطلاب والموظفين؟ بدون بروتوكولات الخصوصية الصحيحة، يمكن لمجرمي الإنترنت السرقة.

قارن حماية الأمن السيبراني لمدرستك بحماية المؤسسات الأخرى. ماذا يفعلون وماذا يجب على المدرسة أن تفعل؟ ثم بمجرد أن يكون لدى المسؤولين فكرة عن الاتجاه الذي يجب أن يسلكوه، يمكنهم الحصول على عمليات تدقيق وتقييم للمخاطر. (الردفاني، محمد قاسم أسعد ،2012 م)

*** ضع خطة**

بناءً على المعلومات المقدمة في خطوة إعادة التقييم، يمكن أن يبدأ التخطيط.

هنا، من المهم أن يناقش المسؤولون والخبراء الفنيون احتياجاتهم مع جميع الإدارات. ما الذي غير التعلم عن بعد؟

ما هي المطالب الجديدة التي يطرحها الفصل الافتراضي؟

تتضمن بعض الأشياء التي يجب مراعاتها الشبكات غير الآمنة وهجمات البرامج الضارة وبرامج الفدية والتصيد الاحتيالي.

ستظهر هذه القضايا وستكون مجالات اهتمام رئيسية. قد تشمل الحلول الشبكات الخاصة الافتراضية (VPN)والبنية التحتية القوية لتكنولوجيا المعلومات.

*** تكوين فريق تكنولوجيا المعلومات**

إذا لم يكن لدى المدرسة فريق تكنولوجيا معلومات بالفعل، فقد حان الوقت لإنشاء ميزانية لهذا الفريق.

إذا تم القيام بذلك من قبل، فقد حان الوقت لتوسيع الفريق .

مع تزايد مخاطر وتهديداتCOVID-19 ، سواء كان الطلاب بعيدون أم لا، فإن فرق تكنولوجيا المعلومات مهمة لمعالجة جميع المشكلات.

يمكن لفرق تكنولوجيا المعلومات استخدام أشكال مختلفة من التكنولوجيا للبحث عن المتسللين والبرامج الضارة وأي فيروسات أخرى.

يجب عليهم تثبيت برنامج مكافحة فيروسات وجدار حماية قوي لحماية شبكة المدرسة. يحتاجون أيضًا إلى دعم فني عام للطلاب الذين يدرسون في المترل. (الردفاني، محمد قاسم أسعد ،2012 م) التواصل ضروري دائمًا.

*** التدريب على التوعية**

التعليم ضروري لأولئك الذين قد لا يملكون حس التقنيين المحترفين.

عندما يصبح الجميع أكثر وعيًا بالتهديدات التي يواجهونها هم والمدرسة، يمكنهم تحديد هذه العلامات مبكرًا.

على سبيل المثال، غالبًا ما تكون حيل التصيد الاحتيالي رسائل بريد إلكتروني مزيفة من شخصيات ذات سلطة.

قد يقدمون روابط ضارة أو يطلبون معلومات خاصة من الأفراد أو المدارس. إذا لم يحدد الطلاب والموظفون رسائل البريد الإلكتروني هذه كرسائل غير مرغوب فيها، فقد ينتج عن ذلك انتهاك.

سيكون توفير الموارد للتدريب، مثل الاختبارات والدروس والممارسات، لا يقدر بثمن. يُعد إنشاء ثقافة الأمن السيبراني في التعليم خطوة قوية، ويجب أن تكون عملية مستمرة للتعلم والتكيف المستمر. البكري، يوسف الشيخ (٢٠١٧)

*** ضبط بمرور الوقت**

١- مثل جميع أنواع التعليم، تتغير ممارسات الأمن السيبراني بمرور الوقت.

٢- جزء مما يجعل أي ثقافة مهمة للغاية هو تطورها - يجب أن يحدث تطور الأمن السيبراني في نفس الوقت.

٣- تتطور التكنولوجيا كل عام، وتظهر أدوات وشبكات جديدة باستمرار. يتكيف مجرمو الإنترنت مع هذه التغييرات ويزدادون ذكاءً.

٤- تتضمن هذه الخطوة المدارس إعادة تقييم وضعها وإجراء عمليات تدقيق وإعادة تقييم المخاطر من وقت لآخر. وهذا من شأنه أن يحافظ على استمرارية الثقافة وسلامة كل فرد فيها.

٥- تطبيق ثقافة الأمن السيبراني في التعليم، يحتاج الجميع إلى وقت للتعود عليها.

٦- سيكون هناك منحنى تعليمي، ولكن طالما يحافظ الجميع على التواصل المناسب، يمكن للمدارس أن تظل آمنة بغض النظر عن المسافة التعليمية. (الردفاني، محمد قاسم أسعد ،2012 م)

*** خاتمة البحث**

يلعب الوعي في مجال الأمن السيبراني دورًا مهمًا في رفع مستوى المعرفة والوعي بين المسؤولين والموظفين وفي ضوء الخطر الوشيك للهجمات الإلكترونية ضد المنظمات والمنشآت الحكومية والحكومية وغير الحكومية لاتخاذ أفضل السبل لضمان حماية البنية التحتية ، لا يقتصر الوعي على الحاجة إلى

حماية البيانات ومنع أساليب الهجمات الإلكترونية ، ولكن أيضًا من خلال زيادة الوعي بكيفية التعامل مع الهجمات الإلكترونية على البنية التحتية وحماية جميع المرافق من الهجمات الإلكترونية ، التي أصبحت تتطور أكثر فأكثر مع تطور التكنولوجيا.

الوعي في مجال الأمن السيبراني هو أحد أسس حماية البيانات والحفاظ على أمن المعلومات وعدم الوقوع ضحية للهجمات الإلكترونية. بل هي الخطوة الأولى في توعية الأفراد والمجتمعات بالمخاطر المتزايدة للهجمات الإلكترونية والعمل على كيفية الرد على الهجمات الإلكترونية، وكسر حواجز الجهل، والقضاء على المعتقدات الكاذبة واللامبالاة. أنماط السلوك غير المبالية وغير الواعية التي يمارسونها بجهل، والتي غالبًا ما تؤدي إلى تدمير البنية التحتية للمنشأة أو الممتلكات العامة والخاصة.

يمكن منع الهجمات الإلكترونية ضد الحكومات والمنظمات، وكذلك ضد الأفراد مثل الوزراء والسفراء والقادة والمسؤولين العسكريين في الدولة، وكذلك المتسللين أو المتسللين الذين يستهدفون رجال الأعمال، طالما أن خبراء الأمن السيبراني بانتظام وفعالية توعية الأثرياء والمدنيين لتحقيق أهدافهم أو للتجنيد لتحقيق مكاسب دولية أو شخصية، نناقش بالتفصيل دوافع ومصالح الدول في مجال الأمن السيبراني، وهي كالتالي:-

الدافع السياسي هو أبرز جهد دولي للتسلل إلى الشبكات الحكومية العالمية أو استهداف القادة الوطنيين. كما تسعى بعض الدول لاختراق الأجهزة الأمنية الحكومية لأسباب سياسية. على هذا النحو، يسعى كبار القادة السياسيين في أي بلد إلى تعزيز الأمن السيبراني لحماية بلدهم ومصالحهم الوطنية وإحباط هجمات العدو.

*** المراجع**

أبو زيد، عبد الرحمن عاطف (٢٠١٩) الأمن السيبراني في الوطن العربي. دراسة حالة المملكة العربية السعودية المركز العربي للبحوث والدراسات على الموقع بتاريخ http://www.alrseg.org/list . aspx?r=24734٢٠٢٠/4/٦ :

٢، البكري ، يوسف الشيخ (٢٠١٧) أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلي مكتبتي جامعة النيلين وجامعة وادي النيل، في المؤتمر الثالث والعشرون لجمعية المكتبات الخاصة، قطر .

أحمد عيسى: بوابة أخبار اليوم العدد الأسبوعي الأربعاء، 18 سبتمبر ٢٠١٩ .

الشيتي، ايناس ابراهيم (٢٠١٩) تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية على جامعة القصيم .

ماجستير غير منشورة، جامعة القصيم د. العتيبي عبد الرحمن بن بجاد (٢٠١٧) دور الأمن السيبراني في تعزيز الأمن الإنساني .

أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية: الهيئة الوطنية للأمن السيبراني: المملكة على الموقع:

عبد القادر محمد فهمي، النظريات الجزئية والكلية في العلاقات الدولية والأمن السيبراني الدولي، عمان – الأردن –

دار الشروق للنشر والتوزيع 2010 – ص 115 .

جبور، منى الأشقر (2012) الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي في امن وسلامة الفضاء السيبراني.

منظمة (الأسكوا) إدارة تكنولوجيا المعلومات والاتصالات (2011 م) بيروت لبنان، الإرشاد الخامس والخاص بحماية حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

جبور، منى الأشقر (2016) السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة.

حجازي، عبد الفتاح بيومي (2007 م) مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، القاهرة: دار الكتب القانونية.

الردفاني، محمد قاسم أسعد (2012 م) الجرائم الخطرة على الأمن العام، ط. الأولى، صنعاء: مكتبة خالد بن الوليد.

الردفاني، محمد قاسم أسعد (2012 م) الجرائم الخطرة على الأمن العام، ط. الأولى، صنعاء: مكتبة خالد بن الوليد.

عبد القادر محمد فهمي، النظريات الجزئية والكلية في العلاقات الدولية والأمن السيبراني الدولي، عمان – الأردن – دار الشروق للنشر والتوزيع 2010 – ص 115 .

طفي، سمير (2011) وآخرون: الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها.

شلوش، نورة (2018) القراصنة الإلكترونية في الفضاء السيبراني'' التهديد المتصاعد لأمن الدول''، مجلة مركز بابل للدارسات الإنسانية المجلد 8 العدد 2

الأمن السيبراني وفئاته وتاريخة – قانون الأمن السيبراني في الأردن لسنة 2019 ص 30 – جامعة الأميرة سيمة .

أبو زيد، عبد الرحمن عاطف (٢٠١٩) الأمن السيبراني في الوطن العربي. دراسة حالة المركز العربي للبحوث والدراسات على الموقع بتاريخ 2/11.

ماجستير غير منشورة، جامعة القصيم د. العتيبي عبد الرحمن بن بجاد (٢٠١٧) دور الأمن السيبراني في تعزيز الأمن الإنساني .