دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات

The role of the school leadership in strengthening cyber security in the government schools for girls in Jeddah from the point of view of teachers

إعداد

فاطمة يوسف المنتشري

Doi:10.33850/jasep.2020.100703

استلام البحث: ٢٢ / ٥ / ٢٠٢٠ قبول النشر: ٢١ / ٦ / ٢٠٢٠

المستخلص :

هدفت الدراسة إلى معرفة دور القياد المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، وتقديم تصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة. واتبعت الدراسة المنهج الوصفي التحليلي، وتم إعداد استبانة مكونة من محورين وهما: دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات، و دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة، وتم تطبيقها على عينة مكونة من ٤٢٠ معلمة في عدد من المدارس الحكومية بمدينة جدة، وأظهرت نتائج الدراسة أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة يتحقق بدرجة موافقة قليلة من وجهة نظر المعلمات. وفي ضوء تلك النتائج تقدمت الدراسة بتصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات والطالبات، وجاءت آليات تطبيقه عبر التنسيق مع الجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية، واشتمل على آليات خاصة بكل من: المعلمات، الطالبات، المعلمات والطالبات معاً، بالإضافة إلى آليات حماية البيئة المادية لشبكة الانترنت.

ABSTRACT:

This study aimed at identifying the role of school leadership in promoting cyber security in the governmental girls schools in Jeddah from female teachers perspective, and presenting a suggested proposal for the school leadership role in

promoting cyber security in the governmental girls schools in Jeddah. The study adopted the descriptive methodology, a questionnaire consisted of two axes was prepared: the role of school leadership role in promoting cyber security for female teachers, the role of school leadership role in promoting cyber security for female students. the questionnaire was applied on a sample consisted of 420 female teachers in some of the governmental schools in Jeddah. The results of the study showed that the role of school leadership role in promoting cyber security for female teachers, and female students achieved with a low degree from the female teachers perspective.In light of these results, the study presented a suggested proposal for the role of school leadership in promoting cyber security among female teachers and female students. the mechanisms for its implementation came through coordination with the competent authorities concerned with cyber security in the Kingdom of Saudi Arabia, and included mechanisms specific to: female teachers, female students, and both of female teachers and female students. and also mechanisms to protect the physical environment of the Internet.

مقدمة :

أدت الثورة الرقمية المعاصرة إلى إيجاد آفاق غير مسبوقة للتواصل وتبادل المعلومات والأفكار والآراء بين ملايين المستخدمين لشبكة الانترنت حول العالم، وانعكس هذا الأمر على كافة مجالات النشاط الإنساني، ومع انتشار الهواتف الذكية والأجهزة الكفية المحمولة، فقد أصبح استخدام شبكة الانترنت أمراً متاحاً لجميع أفراد المجتمع على اختلاف فئاتهم العمرية، وأهداف هذا الاستخدام.

وعلى الجانب الآخر، ومع التدفق المستمر والهائل للمعلومات، واعتماد الملايين حول العالم من أفراد ومؤسسات خاصة وحكومية على استخدام شبكة الانترنت للتواصل الاجتماعي أو إنجاز العديد من المعاملات، فقد ظهر تهديد جديد لهؤلاء المستخدمين، حيث اتجه البعض إلى اختراق شبكات المعلومات، والتلاعب بالمعلومات وإيذاء المستخدمين بصور واساليب متعددة، وذلك فيما يعرف بالجريمة السيبرانية Cyber Crime (Chang et. al., 2013, p.1881).

وإزاء ما ترتب على تلك الجرائم من خسائر مادية واقتصادية واجتماعية، فقد اتجهت العديد من الدول المتقدمة إلى تبني مبادرات هادفة إلى توفير الأمن السيبراني لجميع مستخدمي الانترنت، وخاصة طلبة المدراس، ومنها مبادرة دول الاتحاد الأوربي لوضع مبادئ الاستخدام الآمن لشبكات المعلومات، والإطار الأوروبي للاستخدام الآمن للأجهزة المحمولة، وفي عام ٢٠٠٩ تم إدراج مفاهيم الأمن السيبراني ضمن المناهج الدراسية في ٢٤ دولة أوروبية، وفي الولايات المتحدة تولت وزارة الأمن الداخلي مسؤولية تعزيز ونشر الوعي بالأمن السيبراني ، وفي إطار هذا الاهتمام تم تأسيس التحالف الوطني للأمن السيبراني (Solms & Solms, 2015, p.15).

وعلى الصعيد التربوي أيضاً أطلقت الحكومة الأمريكية المبادرة الوطنية للتربية السيبرانية National Initiative for CyberSecurity Education (NICE)، وجاءت المبادرة نتيجة للتعاون بين وزارة الأمن الداخلي، والمعهد القومي للمعايير والتكنولوجيا National Institute for Standards and Technology (NIST)، بهدف إعداد قوى عاملة في مجال الأمن السيبراني (Wilson, 2014, p.2).

كذلك سعت بعض الدول النامية إلى اتخاذ إجراءات مماثلة لضمان الأمن السيبراني، وواجهت تلك الدول بعض المشكلات التي تتمثل في عدم وجود مبادرة شاملة للأمن السيبراني، ونقص الدعم الكافي، وعدم وجود مبادرات تعليمية قادرة على مواكبة التطورات الحاصلة في مجال الاتصالات وتكنولوجيا المعلومات، وأنعكس هذا الأمر في تراجع مستوى الأمن السيبراني ووقوع مستخدمي الانترنت في تلك الدول أكثر عرضة للهجمات والجرائم السيبرانية (Kortjan & Solms, 2013, p.291).

وفي هذا السياق فقد أكدت العديد من الدراسات على دور المدرسة كأحد أهم المؤسسات التربوية في المجتمع في تعزيز الأمن السيبراني لدى منتسبيها من طلبة ومعلمين، وأشارت دراسة (Goran, 2017) إلى أهمية رفع مستوى وعي الطلبة والمعلمين بالأمن السيبراني، وكيفية الإفادة من شبكة الانترنت بشكل تام، مع تجنب الجرائم السيبرانية التي قد يتعرضون لها اثناء استخدام الانترنت، وأكدت دراسة (Spiering, 2013) على أهمية إعداد خطط لتنمية قدرات أعضاء الإدارة المدرسية والمعلمين في مجال الأمن السيبراني، بهدف نشر وتعزيز الأمن السيبراني في المدرسة والمجتمع ككل، كما أكدت دراسة (المنتشري، ٢٠١٩) على أهمية رفع مستوى الوعي السيبراني لدى المعلمات، والمشرفات التربويات والعاملات في ميدان الإرشاد والتوجيه التربوي.

كما أوضحت بعض الدراسات الدور الهام للقيادة المدرسية في مواجهة الجرائم السيبرانية وخاصة التنمر الإلكتروني، باعتباره أكثر أشكال الجريمة السيبرانية التي تستهدف الطلبة في مختلف المراحل الدراسية، وذلك حسب دراسات (السرحان، ٢٠١٩)، (المساعيد، ٢٠١٧)، و(عبد الرحيم، ٢٠١٧)، وأكدت دراسة "كوريجان وروبرتسون" (Corrigan & Robertson, 2015) على دور القيادة المدرسية في مواجهة الجرائم السيبرانية وتعزيز الأمن السيبراني داخل البيئة المدرسية بشكل عام.

ويتضح مما سبق أن الاهتمام الدولي بتعزيز الأمن السيبراني، في ظل الثورة الرقمية والمعلوماتية المعاصرة، وذلك لمواجهة الجرائم السيبرانية التي تشكل تهديداً جدياً لكافة فئات المجتمع، وللمقدرات الاقتصادية والمادية لكافة دول العالم، كما يتضح الاهتمام الذي أولته تلك الدول للمنظومة التربوية بشكل عام، ولدور المدرسة بشكل خاص في هذا الجانب، كما يتضح الاهتمام بالدور الذي يُمكن أن تؤديه القيادة المدرسية باعتبارها الجهة المسؤولة عن قيادة العمل التربوي داخل البيئة المدرسية.

مشكلة الدراسة

أبدت حكومة المملكة العربية السعودية قدراً كبيراً من الاهتمام بحماية المعلومات والالتزام بمتطلبات الأمن السيبراني، وجاء ذلك في أعقاب تعرض عدد كبير من المؤسسات الحكومية والاقتصادية لهجمات إلكترونية خلال الأعوام الماضية، ومنها استهداف الأنظمة الشبكية لشركة "آرامكو" عام ٢٠١٥، والهجوم على قواعد البيانات الخاصة بوزارة الخارجية، وفي عام (٢٠١٦) تم رصد العديد من الهجمات الإلكترونية التي استهدفت جهات حكومية (الخالد، ٢٠١٨، ص ٥٤).

وإزاء تلك التطورات صدر أمر ملكي كريم رقم (٦٨٠١) في نهاية شهر أكتوبر عام (٢٠١٧) بتأسيس الهيئة الوطنية للأمن السيبراني، بهدف تعزيز الأمن السيبراني وحماية الأمن الوطني والمصالح الحيوية للمملكة، وأحدثت الهيئة تطوراً كبيراً في تعزيز الأمن السيبراني في المملكة، وجاءت المملكة في المركز الرابع عشر عالمياً والأول عربياً في ترتيب المؤشر العالمي للأمن السيبراني Global Security Index (GCI)، الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة (Itu, 2019).

وبالإضافة إلى ذلك فقد أهتمت المملكة بتفعيل دور المؤسسات التربوية في مجال الأمن السيبراني، حيث شهد عام (٢٠١٨) توقيع اتفاقية تعاون بين الهيئة الوطنية للأمن السيبراني ووزارة التعليم ممثلة بوكالة الوزارة لشؤون الابتعاث، وأسفرت تلك الاتفاقية عن إفساح المجال للابتعاث الخارجي في تخصصات (الأمن السيبراني، شبكات الحاسب، والذكاء الاصطناعي)، وتم تخصيص (١٠٠٠) مقعد

لقطاع الأمن السيبراني بواقع (٢٠٠) مبتعث لمدة خمس سنوات، وذلك في أفضل الجامعات الأمريكية والبريطانية والكندية (https://ksp.moe.gov.sa/).

وفي ضوء هذه الجهود، ومع الأخذ في الاعتبار الدور الهام الذي يُمكن أن تؤديه القيادة المدرسية في تعزيز الأمن السيبراني داخل البيئة المدرسية، فقد اتجه اهتمام الدراسة الحالية إلى معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات.

اسئلة الدراسة

تتلخص مشكلة الدراسة في السؤال الرئيس التالي:

ما دور القياد المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات؟

ويتفرع من هذا السؤال الأسئلة الفرعية التالية:

١. ما دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات؟
٢. ما دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة؟
٣. ما التصور المقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة؟

أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف التالية:

١. معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات.
٢. معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة.
٣. تقديم تصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة.

أهمية الدراسة

يُمكن إيجاز أهمية الدراسة على النحو التالي:

١. الدور الهام للأمن السيبراني، كأحد المتطلبات الضرورية لحماية المجتمعات المعاصرة من الجرائم السيبرانية.
٢. تأتي الدراسة استجابة لتوجهات حكومة المملكة العربية السعودية الهادفة إلى تعزيز الوعي بالأمن السيبراني، وإنشاء العديد من الهيئات المختصة العاملة في هذا المجال.
٣. ندرة الدراسات العربية والدراسات التي أُجريت في المملكة العربية السعودية، والتي تناولت دور القيادة المدرسية في تعزيز الأمن السيبراني.
٤. قد تسهم الدراسة في جذب اهتمام الباحثين لإجراء المزيد من الدراسات حول موضوع الأمن السيبراني.

٥. قد تسهم الدراسة في رفع درجة الوعي بأهمية دور القيادة المدرسية في تعزيز الأمن السيبراني داخل المدرسة.

حدود الدراسة

تتمثل حدود الدراسة فيما يلي:

- الحد الموضوعي: تتناول الدراسة موضوع الأمن السيبراني.
- الحد المكاني: أُجريت الدراسة في عدد من المدارس الحكومية بمدينة جدة.
- الحد الزماني: أُجريت الدراسة خلال الفصل الدراسي الثاني من العام الدراسي ١٤٤٠/١٤٤١ هـ.
- الحد البشري: عينة من المعلمات في المدارس الحكومية بمدينة جدة.

مفهوم الأمن السيبراني

يشمل الأمن السيبراني الحد من مخاطر الهجمات والبرمجيات الخبيثة والفيروسات والتي تستهدف البرامج وأجهزة الحاسوب وشبكات المعلومات والاتصالات، واستخدام الأدوات الخاصة بالكشف عن عمليات اختراق الشبكات وإيقاف الفيروسات، وفرض نظم المصادقة وتمكين الاتصالات المشفرة، وعلى هذا يُعرف الأمن السيبراني بأنه "عملية تنظيم وتجميع الموارد والعمليات والهياكل التي تُمكن الفضاء السيبراني من إيقاف عمليات الاختراق بصورها المختلفة، والتي تتم بصورة غير صحيحة قانونية" (Craig, Daikun & Purse, 2014).

وتعرف صائغ (٢٠١٨، ص٢٩) الأمن السيبراني باعتباره "مجموعة الإجراءات التقنية والإدارية والتي تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به للتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف".

ويرى "كانونجيا وماندارينو" Canongia and Mandarino (2014) أن الأمن السيبراني هو "فن ضمان ووجود واستمرارية مجتمع المعلومات، وضمان وحماية الفضاء الإلكتروني، بما يشمل المعلومات والأصول والبنية التحتية الحيوية" كما يُعرف الامن السيبراني بانه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار الى خسائر دائمة (جبور، ٢٠١٢، ص٥).

وفي ضوء ما سبق، يتضح الاتفاق بين الباحثين في أن الأمن السيبراني يمثل مفهوم أمني خاص بحماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو بما يمثل خطرًا على الجهات أو الأفراد ذوي الصلة بتلك المعلومات.

أهداف الأمن السيبراني

تسعى الدول والمؤسسات المختلفة حول العالم إلى تعزيز الأمن السيبراني، وذلك لتحقيق العديد من الأهداف والتي يُمكن إيجازها على النحو التالي (صائغ، ٢٠١٨، ص ٢٢):

- توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.
- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
- توفير المتطلبات اللازمة للحد من الجرائم السيبرانية التي تستهدف المستخدمين.
- مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث إضرار بالغة بالمستخدمين وأنظمة المعلومات.
- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومات والأفراد.
- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها وسد الثغرات في أنظمة المعلومات.

ويشير الربيعة (٢٠١٧) إلى أهداف الأمن السيبراني في المملكة العربية السعودية على النحو التالي:

- ضمان توافر استمرارية عمل نظم المعلومات.
- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة.
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبني التحتية الحساسة فيها.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.
- تعزيز حماية الشبكات وأنظمة المعلومات.
- تعزيز حماية وسرية وخصوصية البيانات الشخصية.
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال.

الأهمية التربوية للأمن السيبراني:

ساهم انتشار استخدام وسائل الوصول إلى شبكة الإنترنت عبر العديد من الأجهزة المحمولة بالإضافة إلى الحواسيب، واعتماد الحياة المعاصرة في معظم مجالاتها على التكنولوجيا الرقمية، على وقوع العديد من المعلمين حول العالم كضحية لأحد أشكال الجرائم السيبرانية، ويترتب على تلك الجرائم العديد من الأضرار المادية والنفسية والمعنوية التي تؤثر على المعلم والمؤسسة التربوية، وهذه الأضرار تُكسب الأمر السيبراني أهمية خاصة بالنسبة لكل معلم في عالم اليوم (Wilson, 2014, p.5).

وتنعكس تلك الأهمية بشكل خاص على طلبة المدارس، باعتبارهم يمثلون الجيل الرقمي، اي الجيل الذي بدأ استخدام تقنيات الاتصال المختلفة منذ سنوات عمره المبكرة، ويزداد أعداد الطلبة مستخدمي الإنترنت بشكل كبير سنويًّا لأغراض متعددة ومنها: التعليم، واللعب، والتواصل الاجتماعي، وتبلغ نسبة الطلبة الذين لديهم إمكانية الوصول إلى الإنترنت نحو ٤٠% من الطلبة حول العالم، وعلى الرغم من مزايا استخدامهم للإنترنت، إلا أن فرص وقوعهم كضحايا للجرائم السيبرانية كبيرة جدًّا؛ لعدم امتلاكهم الوعي الكافي بتلك الجرائم وكيفية تجنبها، وهو ما يزيد أهمية الأمن السيبراني في مجال التعليم والتعلم (Kritizinger, Bada and Nurse,2017, p.5).

وبالإضافة إلى ما سبق من أهمية تربوية للأمن السيبراني للمعلمين وللطلبة، فإن هناك جانب خاص يتمثل في ضرورة ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر، ومتابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة، ومراقبة أي محاولات للتسلل إلى شبكات المعلومات الخاصة بالمدرسة كمؤسسة تربوية (Stewart & Shilingford, 2011, p.8).

الجرائم السيبرانية

يُقصد بالجرائم السيبرانية جميع الأنشطة التي تؤدى بغرض إجرامي في الفضاء السيبراني، وتستهدف هذه الأنشطة ثلاث فئات: الأشخاص، والمنظمات التجارية وغير التجارية، والحكومات (Singh & Singh, 2010, p.1).

وتُصنف الجرائم السيبرانية إلى قسمين: القسم الأول يستهدف الحواسيب وشبكات المعلومات، كالفيروسات والديدان الخبيثة، والقسم الآخر يستهدف مستخدمي الإنترنت ورواد الفضاء السيبراني، ويشمل ذلك الأفراد والمؤسسات الاقتصادية،

والوزارات الحكومية، ومنها التنمر الإلكتروني، والتصيد، والهندسة الاجتماعية، والعديد من الأشكال الأخرى (Tiwari, Anshika, & Ritu, 2016, p.47).

الفيروسات Viruses: وهي برامج حاسوبية خبيثة تتنقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى، وهناك أنواع للفيروسات، ومنها ما يبدأ عمله بوقت أو حادثة معينة، حتى أصبح هناك تقويم للفيروسات التي ستعمل في يوم ما، ومنها ما يكون مكوناً من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري، ومنها ما يكون متخفياً حتى عن برامج مكافحة الفيروسات (الغثبر والقحطاني، ٢٠٠٩، ص٢٨).

وتلحق تلك الفيروسات أضراراً كبيراً ببيئة المعلومات، وقد تصل إلى تدمير جميع الملفات الموجودة على وسائط التخزين، أو استبدال المعلومات بأخرى لا معنى لها، أو إعادة تهيئة القرص الصلب، أو إجراءات تغييرات ذكية وبارعة للبيانات دون أن تترك أثراً يشير إلى التغيير الحاصل، ولن يكون من الممكن اكتشاف الإصابة إلا بعد بضعة أيام وبذلك لا يُمكن الوثوق بالنسخة الاحتياطية أيضاً (عقيل،٢٠١٤، ص١٨).

الديدان الخبيثة Worms: لا تحتاج الديدان إلى برنامج آخر تلتصق به للقيام بدورها، كما هو الحال بالنسبة للفيروس الذي يلزمه حاضن hast لتنفيذ مهمته، ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف إلى آخر، ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار، ولا تعمل الديدان على تخريب الملفات واتلافها كما هو الحال بالنسبة للفيروسات، ولكنها تسبب زيادة عبء على تحميل الشبكة حيث تقوم باستهلاك الذاكرة أو المعالج أو وسائط التخزين أو سائر موارد الحاسوب وشبكة المعلومات، وقد تؤدي إلى توقف النظام (عبد الهادي، ٢٠٠٢، ص١٨).

التنمر الإلكتروني Cyberbullying: يُعد التنمر الإلكتروني من أكثر أشكال الجرائم الإلكترونية انتشاراً بين طلبة المدارس في جميع مراحل التعليم، ويُعرف على أنه شكل من أشكال التحرش يحدث باستخدام تكنولوجيا الاتصالات والمعلومات، ويستطيع المتنمر إيذاء شخص أو مجموعة من الأشخاص بشكل مستمر بصور متعددة (Alhejaili, 2013, p.4).

ويتخذ التنمر الإلكتروني أشكالاً متعددة منها: الإساءة لشخص وتهديده بالإيذاء، الذم والقدح والتحقير، إرسال الصور والفيديوهات غير الأخلاقية، سرقة الحسابات الشخصية أو التطفل عليها، بث خطاب الكراهية أو اتهامات باطلة للتشهير والتخويف والسخرية والابتزاز، التهميش والإقصاء والطرد من نشاط أو مجموعة إلكترونية دون مبررات (الرفاعي، ٢٠١٨، ص١٢٥):

وقد يتسبب التنمر الإلكتروني في معاناة الضحية وإلحاق الأذى البالغ بتقديره لذاته، وشعوره بانعدام الثقة في الآخرين، وعلاقاته الاجتماعية، ومن الجرائم التي وقعت في الولايات المتحدة الأمريكية عام ٢٠٠٦، إقدام فتاة مراهقة على الانتحار بسبب تعرضها للتنمر من قبل صبي آخر يبلغ ١٦ عاماً عبر أحد شبكات التواصل الاجتماعي، وأظهرت نتائج التحقيق في هذه الواقعة، أنها كانت ضحية للتنمر من جارتها البالغة ٤٩ عاماً، وأدعت أنها صبي يراسل الضحية عبر شبكة التواصل الاجتماعي (Alhejaili, 2013, p.6).

الهندسة الاجتماعية Social Engineering: يُطلق عليها علم أو فن اختراق العقول، وشاع هذا الشكل من الجرائم السيبرانية مؤخراً بسبب الانتشار الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني، ويشير هذا المصطلح إلى مجموعة من الأساليب يستخدمها المجرمون في الحصول على المعلومات الحساسة أو إقناع الضحايا المستهدفين بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بهم، وتهدف الهندسة الاجتماعية إلى التركيز على اختراق العقول بدلاً من التركيز على أجهزة الحواسيب وشبكات المعلومات (عبد الصادق، ٢٠١٣، ص٢٠).

تشويه السمعة Denigration: يُشير هذا المفهوم إلى تشويه سمعة الضحية في الفضاء السيبراني، ويُعرف أيضاً بمصطلح Dissing ويعني نشر معلومات غير صحيحة عن شخص آخر عبر الفضاء السيبراني بهدف الإساءة إليه والحط من شأنه، وقد يتضمن نشر صور للشخص المستهدف عبر مواقع التواصل الاجتماعي أو عبر البريد الإلكتروني، بعد تعديلها بواسطة برامج التصميم الرقمي لخدمة أهداف المهاجم (Kowalaski, Limber & Agaston.., 2008, p.19).

القرصنة Hacking: هي عملية الدخول إلى الأنظمة المعلوماتية من طرف أصحاب الخبرة، وهو عادة مبرمجون غير مسموح لهم بالدخول إلى تلك الأنظمة، بهدف كسر الحواجز الأمنية المحيطة بها، ويستغل القراصنة نقاط الضعف في الجوانب الأمنية لمواقع الانترنت، فيحصلون على فرص للدخول إلى البيانات الشخصية للأفراد أو المؤسسات، وقد يستخدم هؤلاء القراصنة أنواعاً من الفيروسات مثل حصان طروادة، بهدف التظاهر أنهم برمجيات مشروعة اعتيادية لغرض الحصول على معلومات من الحاسوب المضيف (قنديلجي والسامرائي، ٢٠٠٨، ص ١٧٧).

التصيد Phishing: يُعتبر من أسهل الجرائم السيبرانية لمجرمي الفضاء السيبراني، ولا يتطلب الامر منهم سوى إنشاء موقع انترنت، وإرسال رسائل عبر البريد الإلكتروني لتبدو كما لو كانت مُرسلة من شركات معروفة لدى الضحايا، وبهذه الطريقة يُمكنهم الإيقاع بالضحايا والحصول على بعض تفاصيل حساباتهم البنكية،

أرقام بطاقة الائتمان، أو بعض التفاصيل الشخصية، وتُعرف هذه الجريمة أيضاً بمصطلح Spoofing (Tiwari et. al., 2016, p.48).

الاستمالة أو التغرير Grooming

ينشأ هذا النوع من الجرائم عندما يحاول أحد الأشخاص البالغين المهتمين بالاستغلال الجنسي للأطفال إقامة علاقة صداقة مع طفل أو مراهق دون الثامنة عشر من عمره، ويتظاهر المهاجم في بداية الاتصال بصغر سنه ومشاركته نفس الاهتمامات مع الطفل الذي يتواصل معه. وتتطور العلاقة بين الطرفين إلى أن يحوز هذا الشخص ثقة الطفل، ويدفعه إلى إرسال صور جنسية ويتبادل معه الرسائل ذات المحتوى الإباحي، وقد يتطور الامر إلى لقاء مباشر بين الطرفين، أو يستغل المهاجم تلك الصور لبثها عبر الانترنت (Krishna, 2019, p.24).

إجراءات تعزيز الأمن السيبراني

هناك العديد من الإجراءات التي يُمكن لكل مستخدم للإنترنت ولرواد الفضاء السيبراني، ومن هذه الإجراءات (Tiwari et. al., 2016, p.48):

١. المحافظة على تحديث جدران الحماية، والتي تمثل أنظمة الدفاع عن البنية التحتية للبيئة المعلوماتية.
٢. التأكد من إعدادات الحاسوب وشبكة الانترنت.
٣. اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.
٤. عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.
٥. استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.
٦. حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
٧. تحديث كلمات المرور بشكل مستمر، على الأقل مرة أو مرتين شهرياً.
٨. عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

وبالإضافة إلى ما سبق من إجراءات عامة، فإن هناك بعض الإجراءات التي يجب اتخاذها من قبل الإدارة التعليمية بمختلف مستوياتها، والقيادة المدرسية على وجه الخصوص، ومنها (Kritzingler & Bada, 2017, p.8):

١. وضع خطط على مستوى المدارس بشكل عام للتوعية بالأمن السيبراني، والتحذير من المخاطر والانتهاكات السيبرانية، بما يشمل الطلبة والمعلمين.
٢. التأكد من تطبيق جميع المدارس لسياسات واضحة بالنسبة للتعامل مع التكنولوجيا الرقمية، بما يشمل الأمن السيبراني، ويجب تعميم تلك السياسات على جميع

المدارس، والإشراف على تطبيقها من قبل بعض الجهات المختصة في وزارة التعليم.

٣. يجب أن يكون لدى المدرسة خطة عمل واضحة للتعامل مع المخاطر والانتهاكات السيبرانية، وأن تتضمن تلك الخطة الجهات والمؤسسات التي يُمكن للمدرسة التواصل معها لمواجهة تلك المخاطر والانتهاكات.
٤. عقد دورات تدريبية لجميع المعلمين في المجالات التالية: الوعي بالأمن السيبراني لدى الطلبة، الاجراءات التي يُمكن للطلبة اتباعها في حال وقوعهم ضحية للمخاطر والانتهاكات السيبرانية.
٥. التعاون مع بعض المؤسسات الأكاديمية كالجامعات، أو المؤسسات الاقتصادية ومؤسسات المجتمع المدني في وضع خطط التوعية بالأمن السيبراني، وتوفير المصادر والدعم اللازم للتدريب ونشر الوعي بالأمن السيبراني.
٦. إشراك الآباء في خطط وبرامج عمل المدرسة ذات الصلة بالأمن السيبراني.
٧. العمل على نشر الاهتمام بموضوع الأمن السيبراني على نطاق واسع، وذلك من خلال عقد ورشات عمل، ندوات، أيام مفتوحة مخصصة للأمن السيبراني، وضع ملصقات أو توزيع كتيبات أو نشرات للتوعية، أو عبر مواقع التواصل الاجتماعي.
٨. إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.
٩. اعتبار الوعي بالأمن السيبراني من المهارات الحياتية اللازمة للطلبة، وإدراجه ضمن القضايا المثارة اثناء التدريس والأنشطة المدرسية.

الدراسات السابقة:

أهتمت بعض الدراسات السابقة بتناول دور القيادة المدرسية في التعامل مع الجرائم السيبرانية داخل المدرسة، وأهتم عدد منها بالتنمر الإلكتروني كأحد أشكال الجرائم السيبرانية الأكثر استهدافاً لطلبة المدارس، ومنها دراسة (السرحان، ٢٠١٩)، والتي هدفت إلى معرفة درجة ممارسة مديري مدارس التربية والتعليم والثقافة العسكرية الأردنية لدورهم في الحد من التنمر المدرسي بالمرحلة الثانوية من وجهة نظر المعلمين، وأعد الباحث استبانة تم تطبيقها على عينة مكونة من (٨٦) معلماً، وأظهرت النتائج أن ممارسة مديري مدارس التربية والتعليم والثقافة العسكرية الأردنية لدورهم في الحد من التنمر المدرسي يتحقق بدرجة متوسطة، كذلك هدفت دراسة المساعيد (٢٠١٧) إلى معرفة سبل مواجهة تنمر الطلبة من وجهة نظر مديري مدارس البادية الشمالية الشرقية في الأردن، وتكونت عينة الدراسة من (١٠٤) مديراً ومديرة، وأظهرت النتائج أن سبل مواجهة تنمر الطلبة من وجهة نظر مديري المدارس جاءت بدرجة تقدير متوسطة، وجاءت سبل المواجهة على الترتيب

التالي: الاعتداء على الممتلكات، المجال الجسدي، المجال اللفظي، المجال الاجتماعي، كذلك هدفت دراسة (عبد الرحيم، ٢٠١٧) إلى تحديد مستوى أهمية دور مديري المدارس الثانوية الفنية بمحافظة الشرقية في مصر في مواجهة التنمر المدرسي من وجهة نظر المعلمين، ووضع نموذج لتفعيل دور مديري المدارس في مواجهة التنمر المدرسي، وأعد الباحث استبانة طُبقت على عينة قوامها (٤٧٣) معلم، وأظهرت نتائج الدراسة نسبة توافر ضعيفة لدور مديري المدارس في مواجهة التنمر، وبلغت هذه النسبة ٣٩% تقريباً، بينما بلغت نسبة أهمية هذا الدور ٨٦% وهي نسبة مرتفعة، وقدم الباحث نموذجاً مقترحاً لتفعيل دور مديري المدارس الثانوية في مواجهة التنمر المدرسي.

وهدفت دراسة "كوريجان وروبرتسون" (Corrigan & Robertson, 2015) إلى معرفة دور قادة المدارس في مواجهة الجرائم السيبرانية، وتم استطلاع آراء تسعة من مديري المدارس الكندية، وشمل الاستطلاع معرفة الجرائم السيبرانية الناتجة عن استخدام الطلبة لمواقع التواصل الاجتماعي، والسلوكيات والسياسات السيبرانية التي تتبعها المدرسة لتعزيز الأمن السيبراني في المدرسة، وأظهرت نتائج الدراسة أن قادة المدارس يؤدون أدواراً متعددة في تعزيز الأمن السيبراني، والتحرك الفوري في حال وقوع أي جرائم سيبرانية، والتنسيق مع أولياء الأمور لمتابعة تلك الجرائم، كما أوضحت الدراسة دور قادة المدارس في وضع سياسات تدعم الاستخدام الآمن للإنترنت، والاستجابة للأحداث السيبرانية التي قد تحدث خارج نطاق المدرسة. كما تطرقت بعض الدراسات بدور القيادة المدرسية في مجال الأمن السيبراني، ومنها دراسة "مارك ونجوين" (Mark & Nguyen, 2017) والتي هدفت إلى الكشف عن فعالية ورش العمل كمجتمعات تعلم مهنية في رفع مستوى الوعي بالأمن السيبراني لدى الآباء والتربويين، وتعزيز الأمن السيبراني في المنزل والمدرسة، وشارك في هذه الورش ٥١ فرد من الآباء والمعلمين والمرشدين التربويين ومديري المدارس في عدد من مدارس ولاية هاواي الأمريكية، وركزت ورش العمل على دور الآباء والمعلمين، ومديري المدارس، ودور المنزل والمدرسة كبيئة لاستخدام الانترنت، وتم إجراء مقابلات مفتوحة مع عينة الدراسة، بالإضافة إلى تطبيق استبانة للكشف عن فعالية تلك الورش في تعزيز الأمن السيبراني، وأظهرت استجابات افراد العينة رضاهم عن المشاركة في تلك الورش، وأهمية التوعية بالأمن السيبراني، وضرورة التعاون بين المنزل والمدرسة لتوفير بيئة انترنت أكثر أماناً للطلبة، كما أظهرت نتائج الدراسة الدور الهام للمعلمين ولمديري المدارس في تعزيز الأمن السيبراني.

واستعرض "هولي وآخرون" (Holly et. al., 2018) نتائج الدراسة التي أجراها مركز أبحاث التعلم في الولايات المتحدة، وشملت عينة الدراسة ٥٠٣ فرد من مديري المدارس ومساعديهم في عدد من المدارس الأمريكية، وتم إعداد استبانة لاستطلاع آرائهم حول استخدام الطلبة للأنترنت وتعرضهم للجرائم السيبرانية، وذلك من حيث الوقت الذي يقضيه الطلبة أمام الشاشة، والتعلم الشخصي عبر الانترنت، واستخدامهم لمواقع التواصل الاجتماعي، وتعليم الحاسوب للجميع، والجرائم السيبرانية، وأعرب أكثر من نصف قادة المدارس عن قلقهم الشديد بشأن استخدام وسائل التواصل الاجتماعي للطلاب خارج المدرسة، والتنمر الإلكتروني، وإرسال محتوى جنسي عبر الانترنت، وعدم قدرة الطلبة على التحقق من موثوقية الأخبار على الإنترنت، وأشارت النتائج إلى أن القيادة المدرسية تواجه تحديات متعددة في العملية التعليمية في عصر الثورة الرقمية والمعلوماتية.

كما تناولت دراسة "سبيرينج" (Spiering, 2013) دور المدرسة والناشرين في التوعية بالأمن السيبراني، وأجرى الباحث مراجعة للأدبيات التي تناولت هذه الموضوعات، ومقابلات مع المعلمين والمعلمات ومدراء المدارس في عدد من المدارس الألمانية، والمختصين في المجال الرقمي، والناشرين التربويين، وأظهرت النتائج وجود أكثر من (٢٠) مشكلة ناتجة عن نقص الوعي بالأمن السيبراني، ومنها تعرض الطلبة لحالات الاستمالة، التحرش الجنسي، والتنمر الالكتروني، بث محتوى غير أخلاقي، والتهديدات المختلفة، والإيذاء الجسدي، وأرجع أفراد العينة تلك المشكلات إلى عاملين رئيسين وهما: غياب رؤية واضحة للتوعية بالأمن السيبراني، وندرة عدد المعلمين المختصين في مجال الأمن السيبراني، وتوصلت الدراسة إلى تقديم خطة مقترحة للتوعية بالأمن السيبراني تشمل تدريب المعلمين وتأهيلهم وتزويد بالمعارف والمهارات ذات الصلة بالأمن السيبراني، وتطوير معارف واتجاهات مدراء المدارس نحو الأمن السيبراني، وتأهيل البنية التحتية الرقمية في المدارس، وتطوير مستوى الإصدارات التربوية التي تتناول موضوع الأمن السيبراني.

ويتضح من تلك الدراسات الاهتمام بدور القيادة المدرسية في التعامل مع الجرائم السيبرانية التي قد يتعرض لها طلبة المدارس، والتأكيد على أهمية قيام القيادة المدرسية بدورها في تعزيز الأمن السيبراني، وتختلف الدراسة الحالية عن تلك الدراسات من حيث الاهتمام بتعزيز الأمن السيبراني لدى معلمات المدرسة، وهو ما لم تتطرق إليه أي من الدراسات السابقة، بالإضافة إلى اقتصار هذه الدراسات على شكل واحد من أشكال الجرائم السيبرانية (التنمر الإلكتروني)، دون الاهتمام بتعزيز الأمن السيبراني لدى طالبات المدرسة بشكل عام، كذلك اختلفت الدراسة الحالية مع

تلك الدراسات من حيث الاهتمام بتقديم تصور مقترح لتعزيز الأمن السيبراني في المدرسة لدى المعلمات والطالبات.

منهجية الدراسة وإجراءاتها

منهج الدراسة: اتبعت الدراسة المنهج الوصفي التحليلي، ويشمل مجموعة من الإجراءات البحثية يقوم بها الباحث لوصف الظاهر المبحوثة معتمداً على جمع الحقائق والبيانات وتصنيفها، ومعالجتها وتحليلها تحليلاً دقيقاً لاستخلاص دلالتها والوصول إلى نتائج وتعميمات عن موضوع الدراسة (عطية، ٢٠٠٩، ص ١٣٨).

مجتمع وعينة الدراسة: شمل مجتمع الدراسة جميع المعلمات العاملات في المدارس الحكومية للبنات بمدينة جدة خلال الفصل الدراسي الثاني من العام الدراسي ١٤٤٠هـ/١٤٤١هـ، أما عينة الدراسة فقد تكونت من ٤٢٠ معلمة، وهن المعلمات اللواتي ابدين الاستجابات التامة على أداة الدراسة.

أداة الدراسة: تم استخدام الاستبانة كأداة لجمع البيانات الدراسة الحالية، وتم تطبيقها إلكترونيا بهدف ضمان سهولة وسرعة الحصول على النتائج، ولسهولة نشر الاستبانة عبر موقع جوجل درايف، بالإضافة إلى أنها طريقة اقتصادية وأقل تكلفة من الاستبانة الورقية التقليدية، وتضمن سهولة إجراء المعاملات الإحصائية، وروعي في إعداد فقرات الاستبانة صياغتها بشكل واضح ولغة سليمة، وتجنب استخدام مصطلحات غير مفهومة أو تحتمل أكثر من تفسير، وألا تكون الفقرات طويلة بشكل يجعل الفقرة غامضة وغير واضحة.

واشتملت الاستبانة على (١٩) فقرة لمعرفة دور القيادة المدرسية في تعزيز الأمن السيبراني، وتكون هذا القسم من محورين: تناول المحور الأول دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات، وتكون من ١٠ فقرات، وتناول المحور الثاني تناول دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة، وتكون من ٩ فقرات.

وتم التأكد من صدق وثبات الاستبانة على النحو التالي.

صدق الاستبانة: تم عرض الاستبانة على مجموعة من السادة المحكمين للتحقق من مدى مناسبة استخدام الاستبانة لتحقيق أهداف الدراسة، ودقة الصياغة العلمية واللغوية لفقرات الاستبانة، ومدى ملائمة كل فقرة للمحور الذي تنتمي إليه، وإجراء ما يلزم من تعديلات، وفي ضوء آراء السادة المحكمين تم حذف بعض الفقرات، وإعادة صياغة عدد من الفقرات الأخرى.

صدق الاتساق الداخلي: للتحقق من صدق الاتساق الداخلي للاستبانة تم حساب معامل الارتباط بين درجة كل فقرة في الاستبانة والدرجة الكلية للمحور الذي تنتمي إليه، وجاءت النتائج على النحو الموضح في الجدول التالي:

Doi:10.33850/jasep.2020.100703

جدول(١): معاملات الارتباط بين درجة كل فقرة في الاستبانة والدرجة الكلية للمحور الذي تنتمي إليه

دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات		دور القيادة المدرسية في تعزيز الأمن السيبراني لدى الطالبات	
رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط
١	٠,٧٤٠**	١١	٠,773**
٢	٠,876**	١٢	٠,877**
٣	٠,841**	١٣	٠,882**
٤	٠,685**	١٤	٠,890**
٥	٠,709**	١٥	٠,657**
٦	٠,735**	١٦	٠,647**
٧	٠,٨17**	١٧	٠,842**
٨	٠,713**	١٨	٠,757**
٩	٠,745**	١٩	٠,657**
١٠	٠,560*		

** تعني مستوى دلالة ٠,٠١ * تعني مستوى دلالة ٠,٠٥

ويتضح من الجدول السابق أن درجة كل فقرة من فقرات الاستبانة ترتبط بمعاملات ارتباط دالة عند مستويي (٠,٠١، و٠,٠٥) مع الدرجة الكلية للمحور الذي تنتمي الفقرة إليه، وتم كذلك حساب معامل الارتباط بين الدرجة الكلية لكل محور من محوري الاستبانة والدرجة الكلية للاستبانة، جاءت النتائج على النحو التالي:

جدول (٢): معامل الارتباط بين درجة كل محور في الاستبانة والدرجة الكلية للاستبانة

محوري الاستبانة	معامل الارتباط
دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات	٠,٨٠١**
دور القيادة المدرسية في تعزيز الأمن السيبراني لدى الطالبات	٠,٧٨٧**

** تعني مستوى دلالة ٠,٠١

ويتضح من تلك النتائج أن الاستبانة تتسم بقدرٍ عالٍ من الاتساق، حيث أن جميع معاملات الارتباط بين درجة كل محور من محوري الاستبانة والدرجة الكلية للاستبانة، معاملات ارتباط ذات دلالة إحصائية.

ثبات الاستبانة: للتحقق من ثبات الاستبانة تم تطبيقها على عينة استطلاعية، لا تشمل عينة الدراسة، وتم حساب معامل الفا كرونباخ للتحقق من ثبات الاستبانة، وجاءت النتائج على النحو الموضح في الجدول التالي:

جدول(٣): نتائج حساب معامل الثبات لأداة الدراسة

مجالات الاستبانة	عدد الفقرات	معامل الثبات
دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات	١٠	٠,٩١٥
دور القيادة المدرسية في تعزيز الأمن السيبراني لدى الطالبات	٩	٠,٩١١
الاستبانة ككل	٢٠	٠,٩٥١

ويتضح من النتائج السابقة أن قيم معاملات الثبات لمحوري الاستبانة وللاستبانة ككل قيم مرتفعة، وتدل على تمتع البطاقة بقدرٍ عالٍ من الثبات.

الأساليب الإحصائية: تم استخدام التكرارات والمتوسطات الحسابية لحساب استجابات عينة الدراسة على فقرات الاستبانة، والانحرافات المعيارية لحساب مدى تشتت تلك الاستجابات، واستخدم معامل ارتباط بيرسون لحساب صدق الاتساق الداخلي للاستبانة، ومعامل الفا كرونباخ لحساب ثبات الاستبانة.

وتم تقدير استجابات أفراد العينة على فقرات الاستبانة وفق مقياس ثلاثي على النحو التالي: درجة الموافقة الكبيرة (٣ درجات)، درجة الموافقة المتوسطة (درجتان)، درجة الموافقة القليلة (درجة واحدة)، وتم تفسير النتائج من خلال تحديد الحد الفاصل للحكم على تقديرات المتوسطات الحسابية الموزونة بناءً على طول الفئة، وذلك كما يلي: المدى= أكبر قيمة (٣) - أصغر قيمة (١) = ٢، وعدد الفئات = ٣، أي أن طول الفئة = ٢ ÷ ٣ = ٠,٦٦، وبذلك تم حساب المتوسط الحسابي الموزون على النحو الموضح في جدول (٤):

جدول (٤): المتوسطات الحسابية لاستجابات عينة الدراسة على فقرات الاستبانة

درجة الموافقة	قليلة	متوسطة	كبيرة
المتوسط	١ – ١,٦٦	١,٦٧- ٢,٣٣	٢,٣٤- ٣

الإجابة عن أسئلة الدراسة

للإجابة عن أسئلة الدراسة تم حساب التكرارات والمتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محوري الاستبانة، ومن ثم بيان درجة الموافقة تبعاً لذلك على كل فقرة في الاستبانة وعلى كل محور على حدة، وفي ضوء تلك الاستجابات تم صياغة التصور المقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني، وفيما يلي عرض لتلك الإجابات.

Doi:10.33850/jasep.2020.100703

إجابة السؤال الأول: نص السؤال الأول على " ما دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات؟"، وتمت الإجابة عن هذا السؤال، حسب استجابات أفراد العينة على النحو الموضح في جدول (٥)

جدول (٥): استجابات أفراد العينة على المحور الأول من أداة الدراسة

م	دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
١	تنظم القيادة المدرسية دورات تدريبية للمعلمات للتوعية بالأمن السيبراني	1.61	0.49	قليلة	٥
٢	توجه القيادة المدرسية اهتمام المعلمات إلى اختيار كلمات مرور قوية للحسابات الشخصية (البريد الإلكتروني، مواقع التواصل الاجتماعي،.....)	1.53	0.54	قليلة	٧
٣	تدعو القيادة المدرسية المعلمات إلى تجاهل العروض والتطبيقات الحاسوبية مجهولة المصدر	1.47	0.5	قليلة	٩
٤	تطلب القيادة المدرسية من المعلمات تحديث كلمات المرور باستمرار.	1.65	0.56	قليلة	٤
٥	تطلب القيادة المدرسية من المعلمات عدم التعامل مع رسائل البريد الإلكتروني مجهولة المصدر.	1.49	0.51	قليلة	٨
٦	توجه القيادة المدرسية جميع مستخدمي الحاسوب في المدرسة إلى عدم ترك الأجهزة مفتوحة دون استخدام.	1.90	0.42	متوسطة	٢
٧	تشرك القيادة المدرسية المعلمات في وضع برامج عملية للتعريف بالأمن السيبراني وآليات تعزيزه	1.٥٥	0.65	قليلة	٦
٨	تنبه القيادة المدرسية المعلمات إلى عدم الافصاح عن بياناتهن الشخصية في الفضاء السيبراني (عبر مواقع التواصل الاجتماعي على سبيل المثال)	1.92	0.64	متوسطة	١
٩	تهتم القيادة المدرسة بتوعية المعلمات	1.71	0.61	متوسطة	٣

	بالجهود الحكومية الهادفة إلى تعزيز الأمن السيبراني				
١٠	تضع القيادة المدرسية ضوابط لحماية الاصول المعلوماتية للمدرسة من الوصول غير المسموح به	1.45	0.50	قليلة	١٠
	المحور ككل	١,٤٥	٠,٥٤	قليلة	

يتضح من النتائج السابقة أن استجابات المعلمات أظهرت درجة موافقة قليلة بشكل عام على دور القيادة المدرسية في تعزيز الأمن لديهن، وجاءت استجابات المعلمات بدرجة موافقة متوسطة على ثلاث فقرات، وجاء في مقدمتها تنبيه القيادة بعدم الإفصاح عن البيانات الشخصية للمعلمات في الفضاء السيبراني، ويأتي ذلك في إطار حرص القيادة المدرسية على عدم انتهاك خصوصية المعلمات، أو تعرضهن للتلاعب بمعلوماتهن الشخصية، ويلي ذلك التنبيه بعدم ترك أجهزة الحاسوب مفتوحة دون استخدام، ويُفسر ذلك ضمن حرص القيادة المدرسية في الحفاظ على الموارد المادية للمدرسة ولشبكة المعلومات، ثم توعية المعلمات بالجهود الحكومية الهادفة إلى تعزيز الأمن السيبراني، وقد يأتي هذا الأمر استجابة لتوجيهات مديريات التربية والتعليم في التوعية بتلك الجهود.

أما باقي الفقرات فقد جاءت الموافقة عليها بدرجة قليلة، وتعكس تلك الاستجابات قلة اهتمام القيادة المدرسية بتعزيز الأمن السيبراني لدى المعلمات، وغياب الكثير من الإجراءات المتعلقة بحماية المعلمات في الفضاء السيبراني، وذلك فيما يتعلق بتحديث كلمات المرور، أو اختيار كلمات مرور قوية، أو عقد دورات تدريبية، وجاء حرص القيادة المدرسية وضع ضوابط لحماية الاصول المعلوماتية للمدرسة من الوصول غير المسموح به في الترتيب الأخير، وهو ما يعني عدم وجود تحديد دقيق للصلاحيات الممنوحة لمستخدمي شبكة المعلومات في المدرسة.

إجابة السؤال الثاني: نص السؤال الثاني على " ما دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة؟"، وتمت الإجابة عن هذا السؤال، حسب استجابات أفراد العينة على النحو الموضح في جدول (٧)

جدول (٧): استجابات أفراد العينة على المحور الثاني من أداة الدراسة

م	دور القيادة المدرسية في تعزيز الأمن السيبراني لدى الطالبات	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
١١	تنظم القيادة المدرسية دورات تدريبية للطالبات للتوعية بالأمن السيبراني	1.43	0.5	قليلة	٨
١٢	تخصص المدرسة أياماً مفتوحة لتعريف الطالبات بمفاهيم ومخاطر	1.53	0.5	قليلة	٦

Doi:10.33850/jasep.2020.100703

	الأمن السيبراني				
١٣	تحث القيادة المدرسية الطالبات على الإفصاح بشكل مباشر عن تعرضهن لأي شكل من أشكال الجرائم السيبرانية لمعلماتهن أو للمرشدة التربوية	1.84	0.66	متوسطة	٤
١٤	تعقد إدارة المدرسية ندوات مدرسية بإشراف معلمات الحاسوب لتوعية الطالبات بالأمن السيبراني	1.47	0.54	قليلة	٧
١٥	تهتم القيادة المدرسية بالتواصل مع الآباء في حال تعرض الطالبات بشكل من اشكال الجرائم السيبرانية	2.43	0.61	كبيرة	١
١٦	توزع القيادة المدرسية نشرات توعوية بأخلاقيات الأمن السيبراني	1.35	0.48	قليلة	٩
١٧	تنبه القيادة المدرسية الطالبات إلى عدم الافصاح عن بياناتهن الشخصية في الفضاء السيبراني (عبر مواقع التواصل الاجتماعي على سبيل المثال)	1.96	0.71	متوسطة	٢
١٨	تحث القيادة المدرسية طالبات المدرسة على تجنب التواصل مع أشخاص مجهولين عبر مواقع الانترنت (عبر الحاسوب أو الهواتف الذكية.....)	1.92	0.61	متوسطة	٣
١٩	تخصص القيادة المدرسية جلسات إرشادية للطالبات اللواتي يتعرضن للمخاطر السيبرانية	1.71	0.54	متوسطة	٥
	المحور ككل	١,٦٣	٠,٦٦	قليلة	

جاءت استجابات المعلمات على المحور ككل بدرجة قليلة، وجاء في مقدمة تلك الاستجابات اهتمام القيادة المدرسية بالتواصل مع الآباء في حال تعرض الطالبات لأي شكل من أشكال الجرائم السيبرانية بدرجة موافقة كبيرة، وأربع استجابات بدرجة متوسطة، وهي بالترتيب التالي: تنبيه الطالبات بعدم الافصاح عن بياناتهن الشخصية في الفضاء السيبراني، حث الطالبات المدرسة على تجنب التواصل مع أشخاص مجهولين عبر مواقع الانترنت، والإفصاح بشكل مباشر عن تعرضهن لأي شكل من

أشكال الجرائم السيبرانية لمعلماتهن أو للمرشدة التربوية، وأخيراً تخصيص جلسات إرشادية للطالبات اللواتي يتعرضن للمخاطر السيبرانية، ويُمكن تفسير تلك الاستجابات في ضوء حرص القيادة المدرسية على القيام بأدوارها الاجتماعية والتربوية والتواصل مع مختلف الأطراف ذات الصلة بالمدرسة كمؤسسة تربوية، كالآباء، والمعلمات والمرشدات التربويات لحل المشكلات التي قد تتعرض لها الطالبات في الفضاء السيبراني، إلى جانب الالتزام بالمسؤوليات التربوية تجاه الطالبات داخل المدرسة، بالإضافة إلى إدراك القيادة المدرسية لما قد تتعرض له الطالبات من مخاطر في الفضاء السيبراني، وذلك مع شيوع استخدام الطالبات في مختلف المراحل العمرية لشبكة الانترنت، والانتشار الكبير للهواتف الذكية والأجهزة الكفية.

وجاءت استجابات المعلمات بدرجة موافقة قليلة على أربع فقرات في هذا المحور، ويُمكن ملاحظة أن هذه الفقرات تتعلق بالدور التوعوي، والخاص باستباق وقوع الطالبات كضحايا للجرائم السيبرانية، وتدور تلك الفقرات حول تنظيم أيام مفتوحة، أو ندوات أو دورات تدريبية، للتعريف بالأمن السيبراني، أو نشرات توعوية للتعريف بأخلاقيات الأمن السيبراني.

وبشكل عام يتضح من استجابات المعلمات اهتمام القيادة المدرسية بتعزيز الأمن السيبراني لدى الطالبات بدرجة أكبر من الاهتمام بهذا الجانب لدى المعلمات، وتتفق هذه النتيجة مع ما سبق وأن تناولته بعض الدراسات السابقة ذات الصلة، حيث أظهرت تلك الدراسات دور القيادة المدرسية في التعامل مع ظاهرة التنمر الإلكتروني بشكل خاص في مختلف المراحل الدراسية، حيث أظهرت نتائج دراسات (السرحان، ٢٠١٩)، (المساعيد، ٢٠١٧) درجة تحقق متوسطة لدور القيادة المدرسية في مواجهة التنمر الإلكتروني، فيما أظهرت نتائج دراسة (عبد الرحيم، ٢٠١٧)، درجة تحقق ضعيفة في هذا المجال، وهو ما يتفق إلى حد ما مع نتائج الدراسة الحالية، كما تتفق تلك النتائج مع ما أظهرته نتائج دراسة "كوريجان وربروتسون" (Corrigan & Robertson, 2015) من حيث التنسيق بين القيادة المدرسية وأولياء الأمور فيما يتعلق بتعرض الطالبات للجرائم السيبرانية، كما تتفق تلك النتائج بشكل عام مع ما أشارت إليه الدراسات السابقة من حيث الحاجة إلى تعزيز الأمن السيبراني داخل المدرسة.

إجابة السؤال الثالث: نص السؤال الثالث على " ما التصور المقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة؟"، وتمت الإجابة عن هذا السؤال بتقديم تصور مقترح على النحو التالي:

مبررات التصور المقترح

١. أهمية تعزيز الأمن السيبراني لدى كافة فئات المجتمع بشكل عام في ظل الثورة المعلوماتية والتدفق الهائل للمعلومات في العصر الحالي.
٢. أهمية تعزيز الأمن السيبراني لدى المعلمات، من حيث توفير الحماية اللازمة لهن في الفضاء السيبراني، وانعكاس هذا الدور على توعية الطالبات بالأمن السيبراني.
٣. أهمية تعزيز الأمن السيبراني لدى الطالبات، لحمايتهن من العديد من أشكال الجرائم السيبرانية، والتي تستهدف الطالبات في مختلف المراحل الدراسية، خاصة في ظل انتشار استخدام شبكة الانترنت، وسهولة الوصول إليها عبر العديد من الهواتف الذكية والأجهزة المحمولة، ونقص الوعي لدى هؤلاء الطالبات بإمكانية تعرضهن للكثير من المخاطر أو وقوعهن ضحية للعديد من الجرائم السيبرانية.
٤. ما أظهرته نتائج الدراسة الحالية بخصوص دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات والطالبات، والذي تحقق بدرجة قليلة لدى كل من المعلمات والطالبة.

أسس التصور المقترح

يستند التصور المقترح إلى ثلاث أسس وهي: الأساس التربوي، الأساس التكنولوجي، والأساس الأمني على النحو التالي:

الأساس التربوي: يؤدي تعزيز الأمن السيبراني لدى المعلمات والطالبات إلى تجنب وقوع الكثير من الجرائم السيبرانية التي تمثل تهديداً مباشراً بالغ الخطر للأسس العقائدية والأخلاقية للمجتمع المسلم، والتي تشمل نشر الأفكار المتطرفة والتشجيع على الإرهاب بصوره المختلفة، وتشمل التشكيك بالمعتقدات الدينية، إلى جانب نشر السلوكيات والأفكار والأخلاقيات الشاذة التي تخالف تعاليم وتوجيهات العقيدة الإسلامية السمحاء.

الأساس التكنولوجي: أصبح تعزيز الأمن السيبراني أمراً حتمياً لجميع أفراد المجتمع المعاصر، بهدف تعزيز الاستخدام الرشيد لمصادر المعلومات المختلفة، والتعاطي مع كافة متغيرات الثورة الرقمية المعاصر بعقلية مستنيرة مدركة لإيجابيات وسلبيات التجوال والتواصل عبر الفضاء السيبراني.

الأساس الأمني: أن تعزيز الأمن السيبراني لا يُمكن أن يتحقق فقط من خلال وجود مؤسسات حكومية تعمل على نشر الوعي بالأمن السيبراني، بل لا بد من تعزيز هذا الدور من خلال جميع المؤسسات العامة والخاصة في المجتمع، وفي مقدمتها المدارس باعتبارها المؤسسة التربوية المسؤولة عن إعداد الجيل الحالي لمواجهة

المتطلبات والتحديات السياسية والاقتصادية والعلمية في عالم الغد، ولا يُمكن أن يتحقق هذا الدور دون قيام كافة الأطراف بالدور المطلوب منها، وخاصة القيادة المدرسية باعتبارها الجهة التنفيذية المباشرة للعمل داخل المدرسة، والمسؤولة بشكل عملي عن تنفيذ البرامج التعليمية والإرشادية.

أهداف التصور المقترح

- فهم الحاجة للأمن السيبراني، وإدراك أن كل شخص يمكن أن يواجه تهديدات مباشرة أو غير مباشرة تتعلق باستخدامه لشبكات المعلومات وأجهزة الاتصال المختلفة في أي لحظة.
- التعرف على مفهوم الأمن السيبراني.
- التعرف على الجرائم السيبرانية التي تستهدف كافة رواد الفضاء السيبراني.
- التعرف على الآثار المترتبة على عدم الوعي بالأمن السيبراني والتعرض للجرائم السيبرانية.
- توضيح الإجراءات اللازم اتباعها لحماية البيئة المادية للمعلومات (جهاز الحاسوب، وسائط التخزين، الهواتف الذكية والأجهزة المحمولة).
- توضيح الإجراءات اللازم اتباعها للاستخدام الآمن لشبكة الانترنت.
- توضيح الإجراءات التي يُمكن اتباعها في حال التعرض لأحد الجرائم السيبرانية.

آليات تطبيق التصور المقترح

يُقصد بها الإجراءات التي يُمكن للقيادة المدرسية اتخاذها بشكل عملي بهدف تعزيز الامن السيبراني لدى المعلمات والطالبات في المدارس الحكومية بمدينة جدة، وتشمل ما يلي:

١. التنسيق مع الجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية

- التنسيق مع الهيئة الوطنية للأمن السيبراني، عبر المركز الوطني الإرشادي للأمن السيبراني لتنظيم أيام مفتوحة وبرامج توعوية للأمن السيبراني داخل المدرسة.
- عقد ندوات تشمل استضافة المختصين في الأمن السيبراني للتعريف بالأمن السيبراني، ومناقشة أهميته وكيفية تجنب الجرائم السيبرانية.
- تنظيم دورات تدريبية للطالبات وللمعلمات بالتعاون مع الجهات المختصة في الجامعات السعودية.

٢. آليات موجهة إلى المعلمات

- إطلاع المعلمات بشكل مستمر على كافة الجهود التي تبذلها حكومة المملكة العربية السعودية، عبر الهيئات المتخصصة، لتعزيز الأمن السيبراني، وخاصة الجهود ذات الصلة بالميدان التربوي.
- إشراك المعلمات في وضع الخطط والبرامج التوعوية الهادفة إلى تعزيز الأمن السيبراني داخل المدرسة.
- تنسيق الجهود بين القيادة المدرسية وأولياء الأمور والمعلمات لمتابعة حالات الطالبات اللواتي قد يقعن ضحية لإحدى الجرائم السيبرانية.
- تحديد الصلاحيات الخاصة بالوصول إلى مصادر المعلومات عبر أجهزة الحاسوب داخل المدرسة، بما يمنع الوصول غير المسموح به إلى قواعد البيانات والمعلومات في المدرسة.

٣. آليات موجهة إلى المعلمات والطالبات معاً

توجيه اهتمام المعلمات والطالبات إلى الالتزام بالإجراءات التالية عند استخدام شبكة الانترنت، والوصول إلى مصادر المعلومات عبر أجهزة الحاسوب أو غير ذلك من وسائل الاتصال:

- تجنب استخدام كلمات مرور ضعيفة لمواقع التواصل الاجتماعي.
- تجنب استخدام نفس كلمة مرور البريد الالكتروني في مواقع التواصل الاجتماعي.
- تجنب كتابة معلومات شخصية عنك وعن أسرتك.
- التأكد من قيود الخصوصية المطبقة عبر مواقع التواصل الاجتماعي.
- تجنب فتح الروابط غير الموثوق بها التي لا تصل عبر مواقع التواصل الاجتماعي، وعدم استقبال ملفات من أشخاص مجهولين.
- عدم فتح رسائل البريد الإلكتروني مجهولة المصدر.

٤. آليات موجهة إلى الطالبات

- عدم المشاركة في أعمال ضارة على الانترنت مثل الإساءة لشخص آخر، أو نشر معلومات غير موثوقة، أو التحريض ضد شخص أو مجموعة معينة.
- تشجيع الطالبات على إصدار نشرات توعوية، وتنظيم مسابقات علمية تتناول الأمن السيبراني والجرائم السيبرانية.
- إبلاغ المعلمات أو المرشدة التربوية بشكل مباشر عن أي تهديد يرد إليهن عبر شبكة الانترنت.

٥. حماية البيئة المادية لشبكة الانترنت

توجيه اهتمام المعلمات والطالبات إلى الالتزام بالإجراءات التالية عند التعامل مع أجهزة الحاسوب ووسائط التخزين وغير ذلك من مكونات مادية داخل المدرسة أو خارجها، أو عند استخدام الهواتف المحمولة والأجهزة الكفية

- التأكد من وجود برامج حديثة مضادة للفيروسات على جهاز الحاسوب، وتحديث تلك البرامج باستمرار.
- فحص جهاز الحاسوب ووسائط التخزين المادية بشكل دوري للتأكد من خلوها من الفيروسات والبرمجيات الخبيثة.
- تحديث برامج التشغيل ومتصفح شبكة الانترنت بشكل دوري.
- عدم تحميل برامج أو تطبيقات من مواقع مجهولة المصدر.
- قراءة التعليمات الخاصة بالبرامج والتطبيقات التي يتم تحميلها قبل الاستمرار ومتابعة تحميل تلك البرامج والتطبيقات.
- عدم ترك جهاز الحاسوب مفتوحاً دون استخدام.

قائمة المراجع

جبور، منى الأشقر (٢٠١٢). الأمن السيبراني: التحديات ومستلزمات المواجهة. *اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني*. جامعة الدول العربية: المركز العربي للبحوث القضائية والقانونية، بيروت، أغسطس ٢٧ – ٢٨.

الخالد، ساري (٢٠١٨). *اتجاهات في أمن المعلومات وأمانها أهمية تقنية التعمية (الشفرة)*. الرياض: العبيكان للنشر والتوزيع.

الربيعة، صالح بن علي (٢٠١٧). *الأمن الرقمي وحماية المستخدم من مخاطر الانترنت*. الرياض: هيئة الاتصالات وتقنية المعلومات.

الرفاعي، تغريد حميد (٢٠١٨). درجة ممارسة وتعرض طلبة المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس. *مجلة العلوم التربوية*. ٤(٣)، ١١١-١٤٥.

السرحان، سيف فارس (٢٠١٩). دور مديري مدارس التربية والتعليم والثقافة العسكرية الأردنية في الحد من التنمر المدرسي. *رسالة ماجستير غير*

منشورة. جامعة آل البيت: كلية العلوم التربوية: قسم الإدارة والأصول التربوية.

صائغ، وفاء بنت حسن عبد الوهاب. (٢٠١٨). وعي أفراد الاسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية*. المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية. ١٤(٣)، ١٨-٧٠.

الصبان، عبير؛ الحربي، سماح (٢٠١٩). إدمان الطلاب على استخدام مواقع التواصل الاجتماعي وعلاقته بالأمن النفسي والتورط في الجرائم السيبرانية. *المجلة الدولية للدراسات التربوية والنفسية*. ٦(٢)، ٢٦٧-٢٩٣.

عبد الرحيم، محمد عباس (٢٠١٧). دور مديري المدارس الثانوية الفنية بمحافظة الشرقية في مواجهة التنمر المدرسي من وجهة نظر المعلمين. *مجلة دراسات عربية في التربية وعلم النفس*. ٨٥، ٢٨٥-٣٦٢.

عبد الصادق، عادل (٢٠١٣). *الفضاء الالكتروني والثورة في شؤون أجهزة الاستخبارات الدولية*. القاهرة: المركز العربي لأبحاث الفضاء الإلكتروني.

عبد الهادي، محمد فتحي (٢٠٠٢). إعداد اختصاصيي المكتبات والمعلومات في بيئة إلكترونية. *الاتجاهات الحديثة في المكتبات والمعلومات*. ٩(١٨)، ١٣-٢٢.

عقيل، عقيل محمد (٢٠١٤). *أساسيات تقنيات المعلومات*. القاهرة: دار النشر للجامعات.

الغثبر، خالد، القحطاني، محمد (٢٠٠٩). *أمن المعلومات بلغة ميسرة*. الرياض: جامعة الملك سعود، مركز التميز لأمن المعلومات.

قنديلجي، عامر؛ السامرائي، إيمان (٢٠٠٨). *شبكات المعلومات والاتصالات*. عمّان: دار المسيرة.

المساعيد، دينا زياد (٢٠١٧). سبل مواجهة تنمر الطلبة من وجهة نظر مديري مدارس البادية الشمالية الشرقية. *رسالة ماجستير غير منشورة*. جامعة آل البيت: كلية العلوم التربوية: قسم الإدارة والأصول التربوية.

المنتشري، فاطمة (٢٠١٩). وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بالأمن السيبراني. *رسالة ماجستير غير منشورة*. جدة: جامعة دار الحكمة: كلية العلوم الصحية والسلوكية والتعليم.

المراجع الأجنبية

Alhejaili, H. (2013). Usefulness of teaching security awareness for middle school students. *Unpublished master thesis*.

New York: Thomas Golisano College of Computing and Information Sciences.

Canongia, C., & Mandarino, R. (2014). Cyber security the new challenge of the information society. In *Crisis Management: Concepts, Methodologies, tools and applications*: 60-80. Hershey, PA: IGI Global.

Chang, Xu; Pei, Shan-shan & Su, Na. (2013). Research on real-time network forensics based on improved data mining algorithm. *Applied Mechanics and Materials*. 380, 1881-1885.

Corrigan, L., Robertson, L.(2015). Inside the digital wild west: how school leaders both access and avoid social media. A paper presented at proceedings of 12th International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2015).

Craigen, D., Diakun, N. & Purse, R. (2014). Defining Cyber security. *Technology Innovation Management Review*. Carleton University, October, pp. 13-22.

Goran, I. (2017). Cyber security risks in public high school. *Unpublished master thesis.* City university of New York: John Jay college of criminal justice.

Holly, K., Sterling, L., Alexandra, H. & Michael, O. (2018). *School leaders and technology: results from a national survey*. Bethesda: Education week researcher center.

Kortjan, N. & Solms, R. (2013). Cyber security education in developing countries: a south African perspective. *Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering*. 119, 289-297.

Kowalski, R., Limber, S. & Agatston, P. (2008). Cyber bullying : bullying in the digital age. United states of America: Blackwell Publishing.

Krishna, G. (2019). *Be a cyber-warrior: beware of cybercrimes*. India: Prowess Publishing.

Kritizinger, E., Bada, M., & Nurse, J. (2017). A study into the cybersecurity awareness initiatives for school learners in south africa and the uk. *10th world conference on information security education*. Rome: May 29-31.

Mark, L. & Nguyen, T. (2017). An Invitation to Internet Safety and Ethics: School and family collaboration. *journal of invitational theory and practice*. 23, 62-75.

Singh, Brijendra & Singh, Hemant, Kumar. (2010). web data mining research: a survey. Paper presented at *Computational Intelligence and Computing Research (ICCIC)*. India, Coimbatore: Dec, 28-29.

Solms. R. & Solms, S.(2015). Cyber safety education in developing countries. *Journal of systemics, cybernetics and informatics*. 13(2), 14-19.

Spiering, A. (2013). Improving cyber saftey awareness education at duch elementary school. *Unpublished master thesis*. Leiden: Leidein university.

Stewart, K., and Shilingford, N. (2011). Cyber girls Sumer camp: Exposing middle school females to Internet security. *Unpublished master thesis*. University of Minnesota.

Tiwari, S., Bhalla, A., & Rawat, R. (2016). Cyber-crime and security. *International journal of advanced research in computer science and software engineering*. 6(4), 46-52.

Wilson, C. (2014). Cybersecurity education the emergence of an accredited academic discipline. *Journal of the colloquium information system security education*. 2(1), 2-13.