



عنوان البحث

الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس وسبل تعزيزه

الفريق البحثي:

نور نضال الأسطل

سارة عبد الناصر الفرا

مرح فادي الأسطل

علا رمزي أبوشاب

شذا أحمد شبير

ختام أنور الفقعاوي

المعلمات المشرفات:

إيمان الاغا

ابتسام محمد صبح

مديرية التربية والتعليم - خان يونس

مدرسة فاروق الفرا الثانوية بنات

السنة الدراسية

2019/2018م

فهرس الموضوعات

رقم الصفحة	البيان
ب	ملخص البحث
1	مقدمة البحث
1	مشكلة البحث
2	أهداف البحث
2	أهمية البحث
3	حدود البحث
3	مصطلحات البحث
4	الإطار النظري
18	الدراسات السابقة
20	منهج البحث
20	مجتمع البحث
20	عينة البحث
20	أدوات البحث
25	نتائج البحث
25	توصيات البحث
27	المراجع
31	الملاحق

ملخص البحث:

يهدف البحث التعرف إلى الأمن الرقمي لدى طالبات الثانوية في مدارس مدينة خان يونس وسبل تعزيزه، وقد استخدمت الباحثات المنهج الوصفي التحليلي، كما تم استخدام المقابلة والاستبانة كأدوات للبحث، وتكونت عينة البحث من عينة عشوائية من طالبات الثانوية مكونة من 42 طالبة، وقد كانت تساؤلات البحث كما يلي:

1. ما مستوى توافر مفاهيم الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس من وجهة نظرهم؟

2. ما مخاطر استخدام التقنيات الرقمية على طالبات المدارس الثانوية في محافظة خان يونس من وجهة نظر المختصين؟

3. ما السبل اللازمة لتعزيز الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس؟
وقد تم التوصل إلى مجموعة من النتائج كان أهمها: أن هناك العديد من المخاطر للتقنيات الرقمية بالرغم من فوائدها المتعددة، وأن هناك وعي ببعض مقومات الأمن الرقمي للتقنيات لدى الطالبات، وإن كانت نسبية من طالبة لأخرى، وأن موقع التواصل الاجتماعي (الفييس بوك) هو أكثر موقع تتم من خلاله عمليات الاختراق، والابتزاز الإلكتروني، والاسقاط، وأن هناك افتقار توعوي لدى أولياء الأمور بضرورة متابعة التقنيات الرقمية التي يمتلكها أبناءهم، ضعف الرقابة العامة على شبكات ومصادر الحصول على الانترنت، وضعف الرقابة العامة على شبكات ومصادر الحصول على الانترنت، وقلة وجود قانون للجرائم الإلكترونية قوي ويتم تطبيقه بشكل فعال للحفاظ على الأمن الرقمي.

توصي الباحثات بضرورة عقد دورات وورش عمل وندوات لنشر ثقافة الأمن الرقمي بين الطالبات وتعزيز مفاهيم الأمن الرقمي ومقوماته وتكثيف الجهود لإيجاد اليات عمل فعالة لقاعدة توعوية شاملة لجميع مستخدمي وسائل التواصل الاجتماعي، وضرورة إيجاد آلية للرقابة بمفهومها الشامل وتقديم المحتوى النافع لمستخدمي وسائل التواصل، وسن قوانين لمكافحة الجرائم الإلكترونية، بحيث يتم معاقبة كل من يقوم بالتحايل أو ارتكاب جريمة.

مقدمة البحث:

يشهد القرن الواحد والعشرون ثورةً في التكنولوجيا، إذ أصبحت تُسيطر بشكل كبيرٍ على الحياة اليومية وتدخل في كل تفاصيلها، سواءً في الحياة العمليّة أو العلميّة، حتى وصل الحال إلى الاستغناء عن بعض الأدوات التقليديّة والاستعاضة عنها بأدوات إلكترونيّة أو تقنيّة من نتاج ثورة التكنولوجيا. استمد العصر الحاضر لقب عصر التقنيّة والتكنولوجيا انطلاقاً من غزو التكنولوجيا جميع مناحي الحياة، وعلى كافّة الأصعدة؛ إذ لم يقتصر على التّواصل فحسب، بل امتدّ ليُصبح أحد وسائل التّعليم الأساسيّة، والعمل، وأكثر بكثير ممّا كان عليه في السّابق، إذ إنّ انتشاره كان محدود النّطاق، إلّا أنّ دائرته بدأت تتّسع حتى ضمتّ جميع مناحي الحياة الإنسانيّة. (الحيارى، 2017).

ومع هذا التطور السريع في عالم التقنيّة أنتج لنا أجهزة الهواتف الذكية ذات القدرات العالية، التي أصبحت بمثابة الكمبيوترات الصغيرة والتي يُعتمد عليها في كثير من أعمالنا اليومية سواء على المستوى الشخصي أو على مستوى الأعمال. والحقيقة أنّ هذه الأجهزة غالباً ما تحتوي على بيانات مهمة جداً منها (أرقام اتصالات، رسائل SMS، رسائل بريدية، صور شخصية، بيانات سرية وأرقام سرية لغالب الحسابات الشخصية منها الحسابات البنكية والبريدية وبرامج التّواصل الاجتماعيّة وأيضاً حسابات لأنظمة أخرى مهمة). ومع الانتشار الواسع لهذه الأجهزة ازدادت في السنوات الأخيرة حالات التعنيف والاختراق والابتزاز، والتعدي على الملكية الفكرية، بسبب ضعف الأمن الرقمي للمدنيين ومستخدمي الشبكات الافتراضية المختلفة. وكما هي العادة في أي مجتمع من المجتمعات حيث لا يخلو من أفراد يمارسون السرقة والتشويه، انطبق ذلك تماماً على المجتمع الرقمي، لذلك كان من المهم لضمان الحماية والوقاية والأمان اتخاذ التدابير اللازمة بهذا الخصوص كما سنتناوله في بحثنا هذا.

مشكلة البحث:

لهذا فقد دعت الحاجة لأن يكون هذا الموضوع محل دراسة وبحث، حيث تتحدد أسئلة البحث في الأسئلة الفرعية الآتية:

1- ما مستوى توافر مفاهيم الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس من وجهة نظرهم؟

2- ما مخاطر استخدام التقنيات الرقمية بما فيها أجهزة الهواتف الذكية على طالبات المدارس الثانوية في محافظة خان يونس من وجهة نظر المختصين؟

3- ما السبل اللازمة لتعزيز الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس؟

أهداف البحث:

تتمثل اهداف البحث فيما يلي:

1. التعرف إلى مدى توافر مفاهيم الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس.

2. الوقوف على مخاطر استخدام التقنيات الرقمية على طالبات المدارس الثانوية من وجهة نظر المختصين.

3. الكشف عن السبل التي من شأنها تعزيز الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس.

أهمية البحث:

لهذه الدراسة أهمية كبيرة بسبب الموضوع الذي تتناوله، وهو موضوع الوعي بالأمن الرقمي، الذي بات في بعض الاحيان يشكل هاجسا لكثير من مستخدمي التقنيات الرقمية.

وقد يفيد البحث كل من:

1- طالبات المدارس الثانوية لتعزيز مفهوم الأمن الرقمي لدى استخدامهن التقنيات الرقمية.

2. تسهم هذه الدراسة في لفت انتباه الأهل والجهات المعنية بمفاهيم الأمن الرقمي، مما يستدعي ضرورة توعية ابنائهم بخطورة استخدام هذه الاجهزة.

3-قد يفيد البحث المؤسسات التوعوية، والشرطية للقيام بحملات توعية مناسبة لمستخدمي هذه التقنيات.

4-قد يفيد البحث باحثين آخرين في تسليط الضوء على هذا المجال لما له من أهمية كبيرة.

حدود البحث:

تتمثل حدود البحث فيما يلي:

1-الحد الموضوعي:

اقتصرت البحث على دراسة الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس وسبل تعزيزه.

2-الحد البشري:

- عينة من طالبات المدارس الثانوية الحادي عشر والثاني عشر.

- مدير العلاقات العامة في شرطة.

4-الحد الزمني:

الفصل الدراسي الثاني للعام الدراسي 1440هـ-2019م.

مصطلحات البحث:

يشتمل هذا البحث على عدد من المفاهيم والمصطلحات، والتي تشعر الباحثات بضرورة تعريفها، وتحديد إجرائياً وفقاً للسياق الذي استخدم فيه هذا البحث.

-وقد عرفته الباحثات على أنه:

القدرة على إدراك الأشياء والحقائق التي تجري من حولنا بشكل يجعل لدينا القدرة على فهمها وتحليلها.

الأمن الرقمي/ هو مزيج من الأدوات والعادات التي يمكن للمستخدمين استخدامها لمنع الآخرين من رصد تحركاتهم على الانترنت سرا، والوصول الى معلوماتهم المخزنة الكترونياً أو اتصالاتهم والعبث بها، والتشويش على أجهزتهم الالكترونية أو برامجهم. (سبيك اب،2019)

- هو حماية الهوية الرقمية الخاصة بك والتي تستلزم من جميع مستخدمي التكنولوجيا توفير كل الاحتياطات لضمان سلامتهم الشخصية وامن وجودهم في الشبكات، ما يشمل الأدوات لتأمين الهوية في عالم الانترنت. (ابتكار، 2016).
- وقد عرفته الباحثات على انه:
- هو الطرق الوقائية التي يقوم بها الشخص من أجل حماية معلوماته وبياناته الشخصية من الاختراق أو التهكير لضمان السلامة الشخصية.
- طالبات المدارس الثانوية: هن طالبات الصفوف الحادي عشر والثاني عشر، والتي تتراوح أعمارهن ما بين 17-18 سنة، واللواتي يتعاملن مع التقنيات الرقمية.

الإطار النظري:

المحور الاول: التكنولوجيا الرقمية

- أ. ماهية التكنولوجيا الرقمية.
- ب. مميزات التكنولوجيا الرقمية.
- ت. مكونات التكنولوجيا الرقمية.
- ث. مجالات استخدام التكنولوجيا الرقمية.
- ج. أهمية التكنولوجيا الرقمية.
- ح. أدوات التكنولوجيا الرقمية.
- خ. سلبيات التكنولوجيا الرقمية.

المحور الثاني: الأمن الرقمي

- ا. تعريف الأمن الرقمي.
 - ب. طرق الاختراقات الأمنية.
 - ب. سبل تعزيز التوعية من مخاطر التقنيات الرقمية.
- أولاً: المحور الأول: التكنولوجيا الرقمية.

تعريف التكنولوجيا الرقمية:

تُعرف بأنها إدارة البيانات، سواء كانت على شكل نص، أو صوت، أو صورة، أو أي شكل آخر، وهي القطاع الذي يتعامل مع الأجهزة والبرمجيات والاتصالات السلكية واللاسلكية في نقل المعلومات وتسهيل عملية التواصل وبالتالي فهو يشتمل على الإنترنت. وتتضمن تكنولوجيا المعلومات معالجة البيانات، نقلها، تبادلها أو استقبالها. (سحيب، 2016)

وفي العصر الحالي يرتبط مفهوم التكنولوجيا ارتباطاً وثيقاً بالتقدم التقني والإلكتروني الذي شهده العالم، وأصبح يعتمد في إنجاز الصناعات والفنون التي يُعبر عنها مُصطلح التكنولوجيا على وجود أجهزة إلكترونية مُتطورة. (الحيارى، 2017).

مميزات التكنولوجيا الرقمية:

وتمتاز التكنولوجيا الرقمية بالخصائص الآتية:

1. سلاسة النظام: حيث تم اختصار العمليات المُعقدة في عمليّات بسيطة، بالإضافة إلى إنجاز مهام مُتعددة في وقتٍ واحدٍ.
2. العالمية والتجانس: ترتبط التكنولوجيا بالحياة العامّة والخاصّة للأفراد والجماعات.
3. . الازدواجية: حيث بإمكانها أن تكون ذات منافع ومضارٍ في نفس الوقت.
4. تأسست وفق قواعد علميّة دقيقة. (شاهين، 2002)

مكونات التكنولوجيا الرقمية:

تتكوّن التكنولوجيا من كلّ ممّا يأتي:

1. المعدّات (Hardware).
2. البرمجيات (Software).
3. قواعد البيانات (Database).
4. شبكات الحاسوب (Networks).
5. العمليّات (Procedure).

أهمية وفوائد التكنولوجيا الرقمية:

تكن أهمية التكنولوجيا الرقمية في انها يمكن الاستفادة منها في مجالات متعددة ومن هذه المجالات:

مجال التعليم والتعلم

لقد قدمت التكنولوجيا خدمة كبيرة في مجال التعليم، بدءاً باختراع القلم والورق، إلى مرحلة الطباعة، ومرحلة التسجيل والتصوير، والآن أصبح الحاسوب من أقوى الوسائط المستخدمة في مجالات التعليم، إضافة إلى استخدام شاشات العرض المختلفة والفيديو وغيرها في التعليم. تعددت الطرق التي وظفت بها تكنولوجيا المعلومات في مجال التعليم والتعلم فاستعملت الوسائط المتعددة (Multimedia)، حتى أصبح بإمكاننا مشاهدة فيلم وثائقي عن كثير من الظواهر الطبيعية كالزلازل والرحلات الفضائية ، ونمو النباتات والكائنات الحية ، واستخدمت البرامج المخبرية التي تظهر محاكاة الواقع الذي تتم به التفاعلات المختلفة بين الذرات والجزيئات ، وعملت التكنولوجيا بذلك على : تقريب البعيد ، وتكبير الصغير ، وتصغير الكبير ، وإظهار أدق التفاصيل دون خوف أو ضرر ، وكذلك التعلم عن بعد حيث يمكن لمتعلم في بلد ما أن يستمع ويناقش محاضراً في بلد آخر وأصبحت الشبكة العنكبوتية (الانترنت) مصدراً أساسياً من مصادر التعليم لا غنى عنه للطالب والمعلم ومصدراً للمعلومة لأي شخص اخر.(عبيات،2018)

مجال الاتصالات

أصبح ممكناً في هذه الأيام أن تشاهد أو تسمع ما يحدث في ابعـد مكان في هذا العالم، فلم يعد الاتصال مقتصرًا على الرسائل البريدية أو المكالمات الهاتفية، فهناك البريد الإلكتروني والدرشة الإلكترونية، وغيرها من الوسائل وكذلك التراسل الفوري للمعطيات أو التحدث مع الآخرين عبر اللقاءات المرئية وذلك بفضل تكنولوجيا الاتصال وشبكات الحاسوب حتى أصبح العالم أشبه بقريـة صغيرة ومن المستجدات إمكانية استخدام شبكة الانترنت لإجراء الاتصالات الهاتفية بتكلفة قليلة من خلال ما يسمى (الصوت عبر بروتوكول الانترنت). VOIP

التجارة الإلكترونية

يقصد بالتجارة الالكترونية القيام بعمليات العرض والبيع والشراء للسلع والخدمات والمعلومات عبر نظام الكتروني بين المنتج والمورد والمستهلك. بحيث تحقق الشركات فوائد عدة منها: تسويق أكثر فاعلية، تقليل عدد الموظفين الذي لم يعد لهم حاجة في الأعمال الإدارية والحسابات، التواصل الفعال مع الشركات الأخرى والزبائن اينما وجدوا.

المجال الإداري

تستخدم المؤسسات الحواسيب والشبكات الداخلية والخارجية في تسيير شؤونها الإدارية وكذلك في التراسل بين فروع المؤسسة التي قد تكون متباعدة ولم يعد مصطلح (المكتب بلا ورق) الذي تنتج فيه المعلومات ويتم تبادلها إلكترونياً بعيد المنال ، كما أصبحنا نسمع في الوقت الحاضر مصطلح الحكومة الالكترونية يتردد كثيراً في وسائل الإعلام .فقد لجأت الدول حديثاً إلى نظام الإدارة الالكترونية الذي يعتمد على تكنولوجيا المعلومات والاتصالات في إدارة نشاطاتها المختلفة ، من خلال أنظمة المعلومات المحوسبة سواء في المستوى الإعلامي أو التفاعلي في التواصل مع الأفراد وبشكل يضمن حماية المعلومات وأمنها مما يسهل انجاز الخدمات والمراسلات بين الجهات الرسمية من جهة ، والمؤسسات والمواطنين من جهة أخرى ، بما يوفر الوقت والجهد والمال.(عبيات،2018)

الصحة والطب

لقد تم توظيف تكنولوجيا المعلومات والاتصالات في مجال الصحة والتطبيب عن بعد، بهدف رفع المستوى الصحي لسكان المناطق النائية والأرياف، مما يقلل من نفقات العلاج والسفر، ويحقق راحة المريض من عناء الوصول لمراكز العلاج المجتمعة في المدن الكبرى، وكذلك التبادل المعرفي بين المراكز الطبية المنتشرة في العالم، عبر المؤتمرات العلمية والطبية المرئية وربط المستشفيات البعيدة بعضها عن بعض بشبكة اتصال تمكن الأطباء من تشخيص الأمراض من خلال تبادل الصور والتقارير وتقديم مشورات طبية في الحالات المرضية المعقدة. إضافة لما سبق تم إنشاء ما يعرف بالصيدلية الالكترونية التي تهتم بتقديم معلومات محددة حول الأدوية وتسويقها عبر الانترنت، كما

يتم عبر البطاقات الالكترونية الخاصة بتسجيل التاريخ الطبي للشخص وأصبح الانترنت مصدراً أساسياً للمعلومات الصحية.

مجال الإعلام والثقافة

أسهمت التكنولوجيا في تقديم خدمة كبيرة في رفع المستوى الثقافي للشعوب، فالورق ثم الطباعة ونتاجها من مطبوعات وكتب وصحف ومجلات والوثائقيات المصورة حول شتى القضايا والنشر من خلال الانترنت أسهمت جميعاً في إيصال المعرفة إلى قطاعات واسعة، ومكنت كذلك الكثيرين من النشر بتكلفة مقبولة. وقد لعبت وسائل الإعلام وما زالت دوراً أساسياً في نقل المعلومة وإيصالها في وقت قريب من حدوثها، سواء كانت مسموعة عبر الإذاعة أو الهاتف أو مسموعة - مرئية عبر البث التلفزيوني وطرق التسجيل الأخرى وحديثاً من خلال الانترنت. وقد اسهمت التكنولوجيا في سهولة توفير المعلومة ومعالجتها وبثها في وقت قصير وترجمتها لعدة لغات.

المجال العسكري:

استخدم الإنسان التكنولوجيا في الحروب فكانت الأسلحة المختلفة عاملاً أساسياً في كسب الحروب قديماً وحديثاً. وكان دور تكنولوجيا المعلومات مهماً في توصيل الرسائل والمعلومات بشكل سري بين القيادة والميدان وكذلك لأغراض التجسس وحديثاً دخلت تكنولوجيا المعلومات المجال العسكري بشكل أوسع فهناك الصواريخ الموجهة بالحاسوب وأنظمة الاتصال الحديثة وغيرها مما أثر بشكل كبير على أداء الجنود في المعركة. (عبيات، 2018)

المجال الترفيهي:

هناك كثير من ألعاب الحاسوب التي يعتمد بعضها على الرسومات الثلاثية الأبعاد والصوت، كما تستخدم تكنولوجيا المعلومات في إنتاج الموسيقى والأفلام والتأثيرات الخاصة المصاحبة لها وتسجيلها وعرضها كما تستخدم الانترنت لتوزيع المنتجات المتعددة الأوساط مما ساعد على انتشارها. (الايداء، 2016)

المجال الصناعي:

صناعة تكنولوجيا المعلومات تشكل قطاعاً مهماً في اقتصاد كثير من الدول وقد استخدم الحاسوب أيضاً في تصميم وفحص نماذج الآلات المعقدة كالسيارات والطائرات كما شاع استخدام الآلات الموجهة بالحاسوب، والإنسان الآلي في الصناعات وخاصة الخطرة منها. وأصبح كثير من الأجهزة يستخدم حواسيب مصغرة لمراقبة عملها، فمثلاً أصبح في السيارة الحديثة عدد من الحواسيب الصغيرة تتحكم في عمل أجزائها المختلفة.

سلبيات التكنولوجيا:

للتكنولوجيا سلبيات عديدة على الفرد والمجتمع، أهمها ما يلي

1. سببت حدوث عزلة اجتماعية في المجتمع، حيث أصبح الأفراد يتواصلون معاً من خلال أسلاك الهاتف وشبكة الإنترنت ومواقع التواصل، وقللوا من تواصلهم في الواقع، مما أثر على السلوكيات الاجتماعية بشكل عام.
2. قللت من قدرة الناس على التفكير والتحليل وإجراء العمليات الحسابية وغيرها من أمور الترجمة والقراءة والبحث عن المعلومات، إذ أن الحواسيب وشبكة الإنترنت قد تكفلت بكل هذه الأمور التي أصبحت متاحة بسهولة، وهذا جعل من العقل البشري اتكالياً بعض الشيء ولا يكلف نفسه عناء التفكير الكبير.
3. أدت إلى زيادة التلوث البيئي وانتشار ظاهرة التصحر واستهلاك الموارد الطبيعية واستنزافها.
4. قللت من الاعتماد على الأيدي العاملة البشرية وزادت من الاعتماد على الآلة مما زاد من نسبة البطالة بشكل كبير.
5. سببت أضراراً كبيرة على الإنسان مثل انتشار الأمراض التي لم تكن موجودة مثل الأمراض الناتجة عن التلوث البيئي، وأمراض السرطان والغدد الصماء.
6. أدت إلى انتشار الحروب وتطور الأدوات المستخدمة فيها، وظهور أسلحة الدمار الشامل والسلاح النووي.

7.زادت من تشتت انتباه الأطفال بسبب زيادة الاعتماد على ألعاب الفيديو وبرامج التلفاز ، مما سبب قلة قدرتهم على التذكر .

8.تسبب الإدمان لمستخدميها بحيث أنهم أصبحوا عاجزين عن أداء العديد من المهمات التي تكفلت بها الآلات. (الحيارى،2017)

أدوات التكنولوجيا الرقمية:

ومن أهم أدوات التكنولوجيا الرقمية:

- الهواتف المحمولة والذكية. -

- الكومبيوتر الشخصي-

- سفن الفضاء -

- الطائرات-

- السفن-

- الغواصات-

- الاقمار الصناعية

- الانترنت-

- الكهرباء السلكية-

- الكهرباء اللاسلكية-

- طابعة ثلاثية الابعاد-

الآلات المستخدمة في كل المجالات مثل المجال الطبي والصناعي-

كذلك هناك آلاف الاختراعات التكنولوجية والتي ساهمت في تغيير العالم بشكل أو بآخر ولن يسعنا الا ان نقول ان التكنولوجيا هي اساس كل شيء حولنا في المنزل او الشارع او العمل او المدرسة.

فالتكنولوجيا هي نتاج وطبيعة تطور المجتمع البشري. (الجمال،2018)

وسنسلط الضوء في هذا البحث على أكثر التقنيات الرقمية استخداما من قبل طالبات الثانوية

العامة وهي (الهواتف الذكية):

باتت الهواتف الجوّالة جزءًا أساسيًا من حياتنا اليومية، إذ لم يعد دورها يقتصر على الاتصال الصوتي والنصي فقط، وذلك نتيجة لأحجامها الصغيرة وأسعارها المنخفضة نسبيًا، وتعدد استخداماتها. ومن هنا سوف نتطرق الى التعرف على الهواتف الذكية.

ما معنى هواتف ذكية:

هو مصطلح يطلق على الهواتف الخليوية التي تعمل بنظام تشغيل، حيث انها تشبه الكمبيوتر الصغير،(عبيات،2018)،وتتيح للمستخدمين إجراء المكالمات الصوتية ، وإرسال الرسائل النصية، وتصفح الانترنت ،وتشغيل العديد من البرامج الأساسية التي يتم تشغيلها في أجهزة الحاسوب، وتشغيل العديد من البرامج الأساسية التي يتم تشغيلها في أجهزة الحاسوب، ومن الجدير بالذكر أنّ الهواتف الذكية تستخدم شاشة تعمل باللمس للتفاعل مع المستخدمين، وتتوفر عليها العديد من التطبيقات والبرامج كالتطبيقات الشخصية والألعاب والبرامج الخاصة المستخدمة في العمل، وقد تم تطوير أول هاتف ذكي غير رسمي سنة 1992م من قبل شركة (IBM)، وفي سنة 1994م تم إصدار نسخة محسنة منه عرفت باسم (Simon Personal Communicator).
(الجمال،2018)

مميزات الهواتف الذكية:

تتميز الهواتف الذكية بالعديد من الميزات الرئيسية، ومنها:

- 1.نظام التشغيل: تستند الهواتف الذكية على نظام تشغيل يتيح لها تشغيل التطبيقات المختلفة، على سبيل المثال تعمل أجهزة الآيفون وفق نظام تشغيل (iOS)، وهواتف البلاكبيرى بنظام تشغيل (BlackBerry OS)، وتعمل أجهزة أخرى وفق نظام الأندرويد والويندوز.
- 2.التطبيقات: تتيح التطبيقات في الهواتف الذكية العديد من الخدمات مثل إنشاء مستندات مايكروسوفت وتعديلها أو عرضها، وتحرير الصور وغير ذلك من الخدمات.

- 3.الاتصال بشبكة الإنترنت: تتيح الهواتف الذكية الاتصال بشبكة الإنترنت بسرعة كبيرة بفضل نمو شبكات الجيل الثالث (G3) والجيل الرابع (G4)، وتتيح للمستخدمين تصفح المواقع المختلفة.
4. لوحة المفاتيح: تتضمن الهواتف الذكية لوحة مفاتيح مدرجة بنفس ترتيب لوحة المفاتيح بأجهزة الحاسوب.
5. إرسال واستقبال الإيميلات: تتيح الهواتف الذكية خدمة إرسال واستقبال الإيميلات والتعامل معها من خلال البريد الإلكتروني، حيث إن معظم الهواتف الذكية تدعم حسابات البريد الإلكتروني المختلفة. (بشار؛2014).

فوائد الهواتف الذكية

للهواتف الذكية العديد من الفوائد، ومنها:

- 1.الخصوصية: تتيح الأجهزة الذكية للمستخدمين خاصية تأمين وتخزين المعلومات الخاصة؛ لاحتوائها على نظام قفل الهاتف، المتاح على شكل رمز، أو كلمة مرور، أو بصمة أصبع، وبالتالي تمنع الدخول إلى إعدادات الجهاز، والتطبيقات المختلفة من دون إدخال كلمة المرور الخاصة، أو الرمز الصحيح، أو بصمة الأصبع.
2. المرونة في التواصل: تتيح الأجهزة الذكية للمستخدمين التواصل مع الأصدقاء والعائلة من أي مكان في العالم بسهولة بمجرد الاتصال بشبكة الإنترنت، سواءً عن طريق ارسال الرسائل، أم الصور، أم مقاطع الفيديو، كما تتيح لهم تصفح مواقع التواصل الاجتماعي، وتسجيل الدخول إلى البريد الإلكتروني والرد على الرسائل، أو وسائل الاتصال الأخرى المتاحة عبر الإنترنت دون الحاجة للجلوس أمام جهاز الكمبيوتر الضخم، وبالتالي إنجاز العديد من المهام بسهولة.
3. التنظيم: تعدّ الأجهزة الذكية أجهزة متعددة الأغراض، فبالإضافة إلى استخدامها كوسيلة اتصال تستخدم كوسيلة للتنظيم؛ لاحتوائها على دفتر عناوين، وآلة حاسبة، وتقويم، ومسجل صوت، وتقويم للملاحظات، والعديد من المميّزات الأخرى التي تنظّم الحياة الشخصية والمهنيّة، كما تساهم في تنظيم المهام، وإتمامها خارج المكاتب؛ لاحتوائها على برامج جداول بيانات، وبرامج قواعد بيانات، وبرامج العرض المتقلّبة.

4. حالات الطوارئ: تظهر فوائد وأهمية الهواتف المحمولة في حالات الطوارئ المفاجئة، فعلى سبيل المثال: يمكن استخدام الهاتف المحمول للاتصال على رقم الطوارئ للإبلاغ عن حصول حادث سيارة أو أي حادث آخر، كما يمكن استخدام تقنية الكاميرا الموجودة في الهواتف المحمولة الجديدة (الهواتف الذكية) لتصوير الحدث، وتوثيق الأدلة.

5. الرعاية الصحية تتميز الهواتف المحمولة الحديثة بفوائدها المختصة بالرعاية الصحية، حيث ساعدت مقدمي الرعاية الصحية، والأطباء عن طريق إتاحة الفرصة لهم لمراجعة الاختبارات، والفحوص الطبية المنزلية في أي مكان، وتقديم العلاجات المناسبة للمرضى، كما مكنتهم من الحصول على فحوصات تنظيم ضربات القلب عن بعد باستخدام الهاتف، وتغيير برمجة الجهاز لمعالجة التغييرات اللازمة للمريض، كما يمكن أن يقوم الأطباء بإجراء بعض التشخيصات المرضية فيما يتعلق ببعض الأمراض عبر الصور المبعوثة للهاتف، وتقديم العلاجات الفورية للمريض وهو في منزله عند حاجته إليها.

6. الحفاظ على البيئة يستخدم معظم الناس مؤخراً تطبيقات الهواتف الذكية لإرسال، واستقبال الرسائل، وتدوين المعلومات والأفكار، وبهذا فإنهم قد استغنوا عن استخدام الأوراق التي تساهم بشكل غير مباشر في تدمير البيئة والغابات.

7. كما تتميز الهواتف الذكية الحديثة بقدرتها على توفير الطاقة، حيث إنّ نظام البطاريات الحديث يقلل من استهلاك الكهرباء، مما يساعد على توفير الطاقة.

8. الترفيه: تعدّ الهواتف المحمولة الحديثة وسيلةً ترفيهية، حيث يمكن من خلالها تشغيل بعض برامج الموسيقى التي تسمح للأشخاص بسماع الأغاني، وتسجيل أصواتهم، بالإضافة إلى تشغيل الفيديوهات التي تتيح للناس فرصة مشاهدة الأفلام، والفيديوهات القصيرة أثناء التنقل، مما يساعد على ترفيه الشخص لنفسه.

9. تتيح للمستخدمين تحديد المواقع الجغرافية بشكل دقيق، من خلال تحديد مكان تواجدهم ومعرفة الطرق.

10. أتاحت لنا الأجهزة الذكية معرفة آخر الأخبار، وحالة الطقس يومياً، والاطلاع على الحجوزات وتوثيقها عن طريق الإنترنت بسرعة فائقة. (عباس، 2013)

سلبيات الهواتف الذكية:

للأجهزة الذكية العديد من السلبيات، ومنها:

1. تُهدّد الخصوصية، وبشكل خاص في حال تعرّض الأجهزة للفقدان، وعدم تأمينها بشكل مناسب.
2. تسبب الإلهاء وفقدان التركيز.
3. تسبب مشاكل صحية، بسبب انبعاث موجات راديوية منها تمتصها أنسجة الجسم، كما أنّ الإفراط باستخدامها يؤدي إلى حدوث مشاكل بصرية.
4. تسبّب الإدمان على تصفّح المواقع الاجتماعية وغيرها من الألعاب. (عباس، 2013)

المحور الثاني: الأمن الرقمي

تعريف الأمن الرقمي: وعرفته الباحثات على أنه هو الطرق الوقائية التي يقوم بها الشخص من أجل حماية معلوماته وبياناته الشخصية من الاختراق أو التهكير لضمان السلامة الشخصية. أو هو حماية الهوية الرقمية الخاصة بك والتي تستلزم من جميع مستخدمي التكنولوجيا توفير كل الاحتياطات لضمان سلامتهم الشخصية وأمن وجودهم في الشبكة، ما يشمل الأدوات لتأمين الهوية في عالم الانترنت.

ففي الحياة الواقعية يقوم الناس بوضع أقفال لأبواب منازلهم، فضلاً عن أجهزة الإنذار، ويمكن عكس المثال ذاته في تحصين وجودنا في الحياة الرقمية.

طرق الاختراقات الأمنية:

قد تعتقد للحظة أن هاتفك أو جهازك غير قابل للاختراق، لكنه فعلاً يمكن أن يخترق وبكل سهولة ودون أن تعرف. وحتى لو لم يتمكن المهاجم الماكر من الولوج إلى هاتفك، فإنه يبقى بإمكانه أن يحصل على المعلومات الحساسة المخزنة فيه، بما في ذلك جهات الاتصال، الأماكن التي قمت بزيارتها والبريد الإلكتروني. (خريشة، 2015)

بينما تالياً ثلاث طرق يتم فيها اختراق أجهزتك الرقمية عادةً:

1. اتصال واي فاي غير آمن:

اتصال واي فاي في الأماكن العامة، مثل المقاهي والمطارات، قد يكون غير آمن، مما يسمح للمهاجمين الاطلاع على كل شيء تقوم به أثناء اتصالك بهذه الشبكة، فمن خلالها يستطيع أحدهم الولوج إلى بريدك الإلكتروني، كلمة السر الخاصة بك، يحاولون الحصول على مدخل لجميع جهات الاتصال لديك، من تقابل، متى وأين. هل توافق؟

تدفق أنظمة التشغيل:

رغم كل النوايا الحسنة لدى مصنعي الأجهزة التقنية، فإن نقاط الضعف تبقى موجودة بحيث تسمح للمهاجمين الفرصة للدخول. وبدورهم مصنعو الأجهزة يقومون بإصدار تحديث نظام التشغيل تكراراً لحماية المستخدمين. ويعلم الهاكرز عن الفجوات الضعيفة ويحاولون اختراق الأجهزة التي لم يتم تحديثها.

تطبيقات البرمجيات الخبيثة:

التطبيقات تضيف الوظائف للأجهزة الذكية، لكنها أيضاً تزيد من خطورة الولوج للبيانات، خصوصاً إذا كنت تقوم بتحميلها من مواقع أو روابط موجودة في رسائل، بدلاً من متجر التطبيقات الرسمي، قد تكون البرمجيات الخبيثة مختبئة داخل التطبيقات، حتى التي تعمل منها، مما يسمح للهاكرز بسرقة البيانات.

وكلما زاد عدد التطبيقات في هاتفك ازداد ما نسميه مساحة سطح الهجوم. وهذا يعني بأن هناك سطوراً برمجية أكثر، وبالتالي هناك احتمال أعلى بأن تحتوي على مشكلة أمنية حرجة.

ممارسات مضرة بالأمن الرقمي:

قد نقوم أحياناً ببعض الممارسات العفوية التي تضر بالأمن الرقمي لأجهزتنا دون معرفة مخاطرها من هذه الممارسات:

فتح المرفقات من مصادر غير معروفة، كما في مرفقات البريد الإلكتروني.-

فتح الروابط العشوائية.

استخدام أجهزة التخزين دون مضاد للفيروسات.

تجاهل المطالبات لتحديث البرنامج.

سبل تعزيز التوعية من مخاطر التقنيات الرقمية:

وهنا سوف نتطرق الى بعض الطرق التي من شأنها حمايتك من مخاطر التقنيات الرقمية، ومن ثم السبل والاقتراحات اللازمة لتعزيز الوعي من تلك المخاطر.

أولاً: نصائح هامة لحماية نفسك من الاختراقات:

استخدام كلمات سرية قوية:

أول طبقة من طبقات الحماية التي يجب عليك استخدامها هي استخدام كلمة سر قوية عبارة عن 14 حرف، أو أن تحتوي على أحرف بجميع الحالات (ويفضل استخدام اللغتين العربية والإنجليزية) وارقام ورموز مختلفة.

بالإضافة الى ذلك لا تضع في الكلمات السرية بيانات مثل تاريخ ميلاد، او اسم أحد المقربين لك مثل زوجة، او أولاد، او غيرهم وذلك لأنه يمكنك للمخترق عن طريق الهندسة الاجتماعية ان يحصل او يخمن الكلمة السرية الخاصة بك.

لا تقم ابدا بالنقر على الروابط المشبوهة:

لا تقم بالنقر على اي رابط يصلك من مصدر مجهول، سواء على البريد الإلكتروني، أو كمنشور على مواقع التواصل الاجتماعي، حيث ان مثل هذه الروابط يمكن ان تقوم باختراق حساباتك، او حتى جهازك الذي تقوم باستخدامه.

هذه الروابط يمكن ان تصلك من مصدر موثوق لك مثل صديق او من موقع مشترك فيه، او البنك الذي يوجد فيه حسابك، وغيرها، ولكنها في الواقع يمكن ان تكون رسائل تصيد زائفة، او أنه قد تم اختراق بريد أو حساب أحد اصدقائك، وتم ارسال مثل هذه الرسائل منه، فيمكن للمخترق ان يقوم بوضع برامج خبيثة بمجرد ان تقوم بزيارة الرابط يتم تحميلها على جهازك، وبالتالي اختراق جهازك.

قم بتحديث نظام التشغيل والبرامج لآخر اصدار :

في كل يوم يتم اكتشاف ثغرات أمنية جديدة في أنظمة التشغيل المختلفة، والبرامج، والتطبيقات، والمتصفحات. بمجرد ان يتم الكشف عن هذه الثغرات فإن المخترقين يقومون بتطوير استغلاليات لهذه الثغرات الأمنية. هذه الاستغلاليات يتم نشرها في الغالب على مواقع ومنتديات المخترقين ويتم اضافتها للبرامج المفتوحة المصدر او المدفوعة والتي يكون الغاية منها هو اختراق هذه الأنظمة او الأجهزة بطرق مختلفة بالاعتماد على الثغرات الأمنية الموجودة فيها.

الشركات المسؤولة عن أنظمة التشغيل والبرامج تقوم وبمجرد اكتشاف الثغرات الأمنية بالبدء بسد هذه الثغرات ومن ثم تصدر تحديثات لها، وهذا ما تلاحظه كل فترة وهو ظهور رسائل لك عن وجود نسخة أحدث من التطبيق او تحديثات للتطبيقات والبرامج او حتى نظام التشغيل الذي تستخدمه، إذا لم تقم بإجراء عملية التحديث هذه فإن اي مخترق يمكنه استغلال هذه الثغرات الموجودة على الجهاز الخاص بك، لذا ننصحك تحديث جميع البرامج الموجودة على الجهاز الخاص بك، والتأكد من أنك تمتلك آخر اصدار محدث.

لا تدخل الى حساباتك بواسطة الأجهزة العامة او مقاهي الإنترنت:

إن عملية استخدامك للإنترنت اللاسلكي المفتوح، او حتى الإنترنت اللاسلكي في المناطق العامة مثل المقاهي، و الفنادق، و المطارات، و غيرها، قد يؤدي الى اختراقك، لأنه يمكن لأي شخص متصل بالشبكة اللاسلكية ان يقوم باختراقك، والتتصت على جميع الاتصالات الخاصة بك عن طريق شن ، وهو هجوم يسمى MiTM هجوم يكون فيه المخترق متوسط للاتصالات بين الشخص المستهدف و الخادم ،ويمكن للمخترق ان يقوم باعتراض الطلبات و تحليلها ،والتعديل عليها، أيضا يمكن لأي شخص حتى و لو لم يمتلك صلاحيات الاتصال بالشبكة أن يقوم باختراق الشبكة، والاتصال بها بشكل غير مشروع، و بالتالي يقوم بعمل ما تم ذكره سابقا ، واستهدافه للأجهزة المتصلة، واختراقها والحصول على البيانات منه.

أضف الى ذلك ايضا بعض الطرق:

لا تقم بتحميل البرامج من مصادر غير موثوقة.

استخدم برامج مكافحة الفيروسات والملفات الخبيثة وابقائها محدثة.

غلق الجهاز والإنترنت في الوقت الذي لا تستخدمهما فيه.

احذف الملفات بشكل آمن قبل بيعك للأجهزة.

لا تستخدم نفس كلمة المرور على حسابات اخرى.

ضع لاصقا على كاميرات الاجهزة في حالة عدم حاجتك لاستخدامها.

ملاحظات مهمة

الحفاظ على الأمن الرقمي ليس شيئاً يمكنك القيام به مرة واحدة ثم نسيانه. بل هي عملية مستمرة تتطلب الوعي الدائم بالتهديدات المحتملة ونقاط الضعف والعمل الاستباقي للتصدي لها. قد تبدو المهمة شاقة، ولكن الفوائد التي ستعود عليك من اتخاذ خطوات لحماية سلامتك وسلامة مصادرك تستحق كل هذا الجهد.

أهم الاقتراحات والسبل الأخرى لتعزيز الأمن الرقمي:

_ نشر ثقافة الأمن الرقمي بين الطالبات وتعريفهم بها.

-عمل حملات توعية، من شأنها أن تعزز مفهوم الأمن الرقمي لدى الطالبات خاصة، والمواطنين عامة هذه الحملات يكون مخطط لها، وتساندها مؤسسات حكومية او أهلية، مثل المؤسسات الشرطية أو مؤسسات حقوق الانسان ومراكز الدعم.

-عقد لقاءات مع أولياء الأمور واطلاعهم على مفهوم الأمن الرقمي وطرق تعزيزه لديهم مما يزيد من حرصهم أثناء استخدام أبنائهم لتلك التقنيات، ومن خلال توضيح النتائج المترتبة على مخاطرها والتي يمكن ان تصل الى حد الاسقاط.

الدراسات السابقة:

لقد قامت الباحثات بالاطلاع على مجموعة من الدراسات السابقة ذات العلاقة بهذا المجال وسوف نذكر ثلاثة من هذه الدراسات:

1.دراسة الجمل (2014) بعنوان: "الآثار السلبية للتقنيات الرقمية على سلوكيات الطلبة من وجهة

نظر المرشدين التربويين ومديري المدارس في جنوب الخليل. " هدفت الدراسة إلى التعرف على الآثار السلبية للأجهزة الذكية على سلوكيات الطلبة من وجهة نظر المرشدين التربويين ومديري المدارس في جنوب الخليل. وقد استخدمت الدراسة المنهج الوصفي التحليلي. وتم استخدام استبانة مكونة من 20 فقرة، موزعة على أربعة جوانب، وبلغ حجم العينة الدراسية (54,2).

ومن أهم نتائج الدراسة ما يلي:

1. إن للأجهزة الذكية آثار سلبية على سلوكيات الطلبة من وجهة نظر المرشدين ومديري المدارس في جنوب الخليل.
2. كما تبين عدم وجود فروق ذات دلالة إحصائية في الآثار السلبية للأجهزة الذكية على سلوكيات الطلبة من وجهة نظر المرشدين ومديري المدارس في جنوب الخليل.
3. دراسة شاهين (2014) بعنوان: "دور الأجهزة الذكية في التفكك الاسري وانحراف الأحداث" هدفت الدراسة إلى التعرف على الدور الذي تلعبه الأجهزة الذكية بالتفكك الأسري بأبعاده الاجتماعية والنفسية والدينية، وبيان دور الأجهزة الذكية على الأحداث من حيث الانحراف الأخلاقي والجنح والجرائم والتعرف على قضية هامة وهي الآثار السلبية للأجهزة الذكية. وقد استخدمت الدراسة المنهج الوصفي التحليلي. وتم استخدام عينة الدراسة 50 فرد من الأخصائيين النفسيين والاجتماعيين وذوي الإعاقة منهم بالأسر المتصدعة والأحداث بمؤسسة الربيع لتأهيل الأحداث بغزة للعام 2014-2015 م. وخلصت الدراسة إلى أن للأجهزة الذكية دور في تحويل الأزواج إلى أفراد فاقدى إحساس ويقلل من حسهم بالمسؤولية تجاه أسرهم.

4. دراسة (قنيفه، 2014) / بعنوان " ممارسات الشباب الجامعي للمواطنة الرقمية عبر شبكات

التواصل الاجتماعي "

هدفت الدراسة الى التعرف على أشكال وطرق ممارسة الشباب الجامعي للمواطنة الرقمية، والتعرف إلى دور الفيسبوك في تبني الشباب الجامعي لسلوكيات جديدة، وقد تمثل مجتمع الدراسة وعينته في الشباب الجامعيين وقد استخدمت الباحثة المنهج الوصفي، وتوصلت الدراسة الى مجموعة من النتائج كان أهمها: كشف الطرق التي يمارس الشباب الجزائري للمواطنة عبر بعض المجموعات الفيسبوكية. وعرض الآراء حول المواطنة الرقمية بشكل عام.

منهج البحث:

لقد استخدمت الباحثات المنهج الوصفي التحليلي، وذلك لأنه يناسب هذا النوع من الأبحاث، وقد عرفت الباحثات المنهج الوصفي على أنه: " هو طريقة لدراسة الظواهر أو المشكلات العلمية من خلال القيام بالوصف بطريقة علمية ومن ثم الوصول الى تفسيرات منطقية لها دلائل وبراهين تمنح الباحث القدرة على وضع أطر محددة للمشكلة ويتم استخدام ذلك في تحديد نتائج البحث ".

مجتمع البحث وعينته:

أ. مجتمع البحث: جميع طالبات المدارس الثانوية في خان يونس.

ب. عينة البحث: تم اختيار عينة عشوائية من طالبات المدارس الثانوية في مدينة خان يونس.

أدوات البحث:

وقد استخدمت الطالبات في هذه الدراسة الأدوات الآتية:

1. المقابلة:

وتعتبر المقابلة من أدوات البحث العلمي عندما يستخدمها الباحث في جمع المعلومات من ذوي العلاقة لتوضيح بعض الامور حول موضوع معين.

1. صياغة أسئلة المقابلة:

كانت أسئلة المقابلة عبارة عن أسئلة مفتوحة تمت صياغتها من قبل الباحثات، كما سيتم ارفاقها في ملحقات البحث ملحق (2).

ب. الهدف من المقابلة:

هدفت الباحثات من خلال المقابلة الى الاجابة عن السؤالين الثاني والثالث من مشكلة البحث وقد كانت أسئلة المقابلة كالتالي:

1. حدثنا عن المخاطر الأمنية للتقنيات الرقمية؟ وبرأيك ماهي أكثر تلك المخاطر التي تتعرض لها الفتيات من وجهة نظرك؟
2. برأيك ماهي الطرق والاحتياطات الأمنية التي يمكن أن تقوم بها الفتيات لتقليل تلك المخاطر الى أدنى درجة ممكنة.
3. أنتم كمؤسسة أمنية وشرطية تابعة لوزارة الداخلية هل كان لكم دور في نشر الوعي الأمني والثقافة الأمنية للتقنيات الرقمية بين المواطنين، وهل ارتقى دوركم الى الدرجة المطلوبة؟

نتائج المقابلة:

وقد تبين من خلال المقابلة

_ أن هناك العديد من السلبيات للتقنيات الرقمية بسبب الاستخدام السيء لها ومن ضمن هذه السلبيات:

العزلة الاجتماعية، التفكك الأسري، كثير من حالات الطلاق، مشكلة العنوسة.
كما تم التطرق الى الكثير من المخاطر بدءا من خدش الحياء العام، والابتزاز الالكتروني وانتهاء بالإسقاط في وحل العمالة والتخاير مع العدو.
كما أوضح أن أكثر المخاطر التي تتعرض لها الفتيات هي الابتزاز الالكتروني، وان أغلب تلك الابتزازات كانت نتيجة موقع التواصل الاجتماعي (الفييس بوك)، وكانت تلك الابتزازات

إما عن طريق الاختراق لأجهزة الضحية، أو من خلال التعرف عليها واستدراجها. وأنه قد تم التعامل مع الكثير من تلك المشاكل وحلها بشكل سري لحساسية الموضوع.

وقد أوعز أن سبب هذه المخاطر وارتفاعها هو:

_ضعف الرقابة العامة على شبكات ومصادر الحصول على الانترنت، وانخفاض تكلفتها الأمر الذي جعلها في متناول الجميع.

-قلة وجود قانون للجرائم الالكترونية قوي ويتم تطبيقه بشكل فعال للحفاظ على الأمن الرقمي.

_قلة متابعة أولياء الأمور لبناتهم بشكل جيد، واعطاءهم مساحة كبيرة من الحرية لاستخدام تلك التقنيات كما يحلو لهن.

-افتقار العديد من الفتيات لبعض مقومات الأمن الرقمي التي من خلالها يمكن حماية أنفسهن ومعلوماتهن الشخصية.

-إضافة الى ضعف الوازع الديني لبعضن، وتغلب شيطان الخلوات عليهن.

كما انه تم التوصل الى بعض الطرق والوسائل الواجب اتباعها لضمان الحماية الشخصية والحد من تلك المخاطر:

- 1.عدم ترك الجهاز مع أي شخص غير موثوق به، أو إعارته لأحد.
- 2.عدم عمل أي صيانات للجهاز بالخارج، وعدم بيعه، لأنه يمكن لأي شخص استعادة أي بيانات سابقة عليه حتى لو تم حذفها.
- 3.التقليل قدر الامكان من استخدام وسائل التواصل الاجتماعي، وعدم حفظ أي معلومات أو بيانات عليها.
- 4.الابتعاد عن شبكات الانترنت المفتوحة وغير الموثوق بها، والتي قد تكون طعم في بعض الاحيان للإيقاع بالضحية.
5. وضع لاصق على الكاميرا طول فترة استخدام الجهاز، وفي حالة عدم الحاجة للكاميرا.

6. تنمية الثقافة الرقمية لدى مستخدمي التقنيات الرقمية لأخذ الحذر، وتجنب مخاطرها وصولاً إلى الحماية الشخصية.

ج. العينة المستهدفة:

استهدفت المقابلة المقدم: نضال كلاب (ابو المثنى) مدير شرطة خان يونس

2. الاستبانة:

ويتم من خلالها الاعتماد على جمع المعلومات بالإجابة على مجموعة من الأسئلة التي يتم تحليلها واستخراج النتائج منها.

وقد عرضت الاستبانة في هذه الدراسة على مختصين لتحكيمها وإبداء ملاحظاتهم عليها، وقد أبدوا ملاحظاتهم، وأخذ بها بعين الاعتبار.

أ. الهدف من الاستبانة:

هدفت الباحثات من خلال تطبيق الاستبانة الاجابة عن السؤال الأول وهو:

1. ما مستوى توافر مفاهيم الأمن الرقمي لدى طالبات المدارس الثانوية في محافظة خان يونس من وجهة نظرهم؟

ب. محاور الاستبانة:

وقد كانت الاستبانة مكونة من محور واحد ايجابي يتناول الاحتياطات الأمنية عند استخدام الأجهزة الذكية.

ج. صياغة فقرات الاستبانة:

تم إرفاق الاستبانة في ملحقات البحث، ملحق (4).

د. العينة المستهدفة: عينة عشوائية من طالبات الثانوية (الحادي عشر، والثاني عشر).

بلغ عدد العينة: 42 طالبة.

وبعد تطبيق الاستبانة، فيما يلي تحليل لنتائجها:

الرقم	الفقرة	درجة كبيرة	درجة متوسطة	درجة قليلة	المجموع
1	أستخدم كلمة مرور خاصة بي ومكونة من أكثر من 14 حرف.	33	30	16	79

86	16	16	54	أبتعد عن استخدام نفس كلمة المرور على حسابات أخرى.	2
104	7	10	87	أتجنب فتح الاعلانات المشبوهة التي عادة ما تكون مرتبطة ببعض التطبيقات.	3
76	23	14	39	أقوم باستخدام برنامج مضادة للفيروسات.	4
60	31	8	21	أضع لاصقا على الكاميرا أثناء استخدامي لهاتفني.	5
98	10	16	72	أتجنب إضافة أي أشخاص على شبكات التواصل الاجتماعي الخاصة بي ان كنت غير متأكدة من هويتهم.	6
88	15	16	57	أقوم بإغلاق شبكة الواي فاي مباشرة بعد الانتهاء من حاجتي لها.	7
89	13	22	54	أبتعد عن فتح الروابط التي تحوي المعلومات المثيرة.	8
95	10	22	63	أتجنب نشر صوري على مواقع التواصل في المناسبات.	9
111	5	10	96	أبتعد عن ترك هاتفي مع أي شخص غير موثوق به.	10
100	7	24	69	أتجنب فتح المرفقات من مصادر غير معروفة.	11

ويتضح من الجدول السابق ما يلي:

1. تبين أن الفقرات الحاصلة على اعلى تكرارات هي الفقرات (3، 10)،

حيث حصلت الفقرة رقم (3) والتي تنص على " أتجنب فتح الاعلانات المشبوهة التي عادة ما تكون مرتبطة ببعض التطبيقات" على أعلى مجموع تكرارات ويساوي 104 تكرار .
وتليها الفقرة رقم (10) والتي تنص على "أبتعد عن ترك هاتفي مع أي شخص غير موثوق به" على مجموع تكرارات 100 تكرار .

وتعزي الباحثات حصول هاتين الفقرتين على أعلى تكرار إلى وجود مستوى من الوعي لدى الطالبات بخطورة الاعلانات المشبوهة، وماجد يترتب عليها من اختراقات وفيروسات للأجهزة الذكية خاصة بعد تعرض بعضهم لمثل تلك المخاطر، بالإضافة الى وعيهم أيضا بخصوصية هذه الأجهزة وأنه لا بد من عدم تركها مع أي شخص غير موثوق به لكثرة الملفات الخاصة جدا التي تحتويه كالصور العائلية وكلمات السر وغيره.

2. كما تبين من خلال تحليل الاستبانة أن الفقرات الحاصلة على أدنى مجموع تكرارات هي الفقرات (4، 5)

حيث حصلت الفقرة رقم (5) والتي تنص على " أضع لاصقا على الكاميرا أثناء استخدامي لهاتفي" على أدنى مجموع تكرارات ويساوي 60 تكرار .
وحصلت الفقرة رقم (4) والتي تنص على " أقوم باستخدام برنامج مضادة للفيروسات" على مجموع تكرارات 76 تكرار .

وتعزي الباحثات حصول هاتين الفقرتين على أدنى تكرار إلى افتقار الطالبات لبعض مقومات الأمن الرقمي مثل جهلن بالمخاطر التي قد تتسبب من وراء ترك الكاميرا دون لاصق في حال عدم حاجتها، على أساس انها تستخدم للتصوير فقط في حال استخدامها، الأمر الذي قد يشكل ثغرة من الممكن لبعض الذئاب البشرية استغلالها بشكل مؤذي من خلال التكبير والاختراق والابتزازات.

اضافة الى جهلن بضرورة وجود برنامج مضاد للفيروسات يحمي الأجهزة من البرامج الخبيثة التي من شأنها تسجيل كل التحركات والملفات والمعلومات الخاصة بالشخص ومراقبتها والحصول عليها.

نتائج البحث:

مما سبق كله نلاحظ أن النتائج التي تم التوصل اليها كالتالي:

1. أن هناك العديد من المخاطر للتقنيات الرقمية بالرغم من فوائدها المتعددة.
2. أن هناك وعي ببعض مقومات الأمن الرقمي للتقنيات لدى الطالبات، وان كانت نسبية من طالبة لأخرى مثل الوعي بمخاطر فتح الروابط المشبوهة المرافقة لبعض التطبيقات، والوعي بعدم ترك الاجهزة الذكية مع أي شخص غير موثوق به، اضافة الى الجهل ببعض المقومات الأخرى كالجهل بمخاطر ترك كاميرا الجهاز دون وضع لاصق عليها، والجهل بأهمية وجود برامج مكافحة للفيروسات.

3. أن موقع التواصل الاجتماعي (الفييس بوك) هو أكثر موقع تتم من خلاله عمليات الاختراق، والابتزاز الإلكتروني، والاسقاط.
4. أن هناك افتقار توعوي لدى أولياء الأمور بضرورة متابعة التقنيات الرقمية التي يمتلكها أبناءهم.
5. ضعف الرقابة العامة على شبكات ومصادر الحصول على الانترنت.
6. عدم وجود قانون للجرائم الإلكترونية قوي ويتم تطبيقه بشكل فعال للحفاظ على الأمن الرقمي.

توصيات البحث:

لقد خرجت الباحثات من هذا البحث بعدد من التوصيات:

1. توصي الباحثات بضرورة عقد دورات وورش عمل وندوات لنشر ثقافة الأمن الرقمي بين الطالبات وتعزيز مفاهيم الأمن الرقمي ومقوماته، لتحقيق النفع والفائدة من خلال الاستخدام الأمثل للتقنيات الرقمية للاستفادة من التكنولوجيا الحديثة بكافة أشكالها.
2. التأكيد على أهمية دور الأسرة الواعية، وأولياء الأمور في متابعة أبنائهم وتوجيه سلوكياتهم وتعزيز هذا الدور من خلال عقد ندوات لهم حول هذا الموضوع.
3. ضرورة تكثيف الجهود مع جميع الجهات مثل المراكز المختصة، ومؤسسات الداخلية، والمدارس الثانوية وأولياء الأمور وعلى جميع المستويات لإيجاد آليات عمل فعالة لقاعدة توعوية شاملة لجميع مستخدمي وسائل التواصل الاجتماعي والانترنت بصفة عامة لتعريفهم بمنافع ومضار هذا التطور التقني.
4. إيجاد آلية للرقابة بمفهومها الشامل وتقديم المحتوى النافع لمستخدمي وسائل التواصل والانترنت عموماً.
5. سن قوانين لمكافحة الجرائم الإلكترونية، بحيث يتم معاقبة كل من يقوم بالتحايل أو ارتكاب جريمة
6. ضرورة القيام بمزيد من الأبحاث التي تتناول هذا الموضوع.

المراجع:

- 1.دراسة (الجمال، سليمان)"الآثار السلبية للتقنيات الرقمية على سلوكيات الطلبة من وجهة نظر المرشدين التربويين ومديري المدارس في جنوب الخليل"، الخليل، فلسطين،2014.
- 2.دراسة(باسم أسماء، عبد الرحمن إيمان). "التأثيرات السلبية لاستخدام الأجهزة الذكية على الأطفال من وجهة نظر الأمهات " 2017.نابلس، فلسطين.
- 3.دراسة (شاهين، سهيلة) "دور الأجهزة الذكية في التفكك الاسري وانحراف الأحداث"،2014.
- 4.دراسة (قنيفه، 2014) / بعنوان " ممارسات الشباب الجامعي للمواطنة الرقمية عبر شبكات التواصل الاجتماعي.الجزائر،2014.
5. (المسقطي، محمد)، "أمن الهواتف التي تعمل بنظام أندرويد ". كتيبات تعليمية. يوليو 2017.
6. موقع ويكيبيديا "تكنولوجيا الاتصال الرقمي"

[%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-](#)

[%D9%81%D8%A7%D9%86%D8%AA%D8%A8%D9%87-%D8%A3%D9%86/#](#)

12. (الحيارى، إيمان)، " ايجابيات وسلبيات التكنولوجيا"، ديسمبر، موقع موضوع، 2017

https://mawdoo3.com/%D8%A5%D9%8A%D8%AC%D8%A7%D8%A8%D9%8A%D8%A7%D8%AA_%D9%88%D8%B3%D9%84%D8%A8%D9%8A%D8%A7%D8%AA_%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7?fbclid=IwAR1vxMaPQbp8tQDkM9PxeJ5zBkdAZaoexCYeeih5v-0BnvbttNQ9OVEhvgU

13. (الجمال، محمد). " ما هي الهواتف الذكية". موقع موضوع. آخر تحديث: ٠٩:٤٢، ١٩ فبراير

٢٠١٨

https://mawdoo3.com/%D9%85%D8%A7_%D9%87%D9%8A_%D8%A7%D9%84%D9%87%D9%88%D8%A7%D8%AA%D9%81_%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9

14. (الاستاذ، سليم). "دراسة انتشار الهواتف الذكية يترافق مع المخاطر الأمنية"، 12 يونيو 2011

<https://arabic.arabianbusiness.com/technology/2011/jun/12/55523>

15. (مروان، محمد). "الوعي". موقع موضوع. آخر تحديث: ٠٩:٣٤، ١٩ يوليو ٢٠١٨

https://mawdoo3.com/%D9%85%D8%A7_%D9%87%D9%88_%D8%A7%D9%84%D9%88%D8%B9%D9%8A?fbclid=IwAR1ulJSIaWoRwO_GGghH5NBR3Y6m1X5LyuUMvbslg5EnYfCM0g3yEwFY7qk

16. (الشوابكة، مراد) "فوائد الأجهزة الذكية" موقع موضوع، آخر تحديث: ١٣:٤١، ٢٧ سبتمبر

"٢٠١٨

https://mawdoo3.com/%D9%81%D9%88%D8%A7%D8%A6%D8%AF_%D8%A7%D9%84%D8%A3%D8%AC%D9%87%D8%B2%D8%A9_%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9

17. مؤسسة مونتي كارلو الدولية. المخاطر الأمنية للهواتف الذكية" آخر تحديث: 2013/04/13
- 11:22

<https://www.mc-doualiya.com/articles/20130412-%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D8%A3%D9%85%D9%86-%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%A7%D9%84%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9-%D8%AA%D8%B3%D9%84%D9%84-%D8%AA%D8%B9%D9%82%D8%A8-%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA>

18. (سعيد، بشار)، "أمن الهواتف الذكية"، مركز مجتمع الأمن العربي، 30 أغسطس، 2014،
<http://security4arabs.com/2014/08/30/smart-mobile-security/>

19. (الإيذاء، سامي)، "الأجهزة الذكية. المخاطر والحماية"، المجموعة السعودية لأمن
المعلومات، 2019

<http://hemayagroup.org/home/%D8%A7%D9%84%D8%A3%D8%AC%D9%87%D8%B2%D8%A9-%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D9%88-%D8%A7%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-2/>

20. (عبيات، علا)، "ما معنى الهواتف الذكية". موقع موضوع، آخر تحديث: ٣٩:١٣، ٢٧
سبتمبر ٢٠١٨

https://mawdoo3.com/%D9%85%D8%A7_%D9%85%D8%B9%D9%86%D9%89_%D8%A7%D9%84%D9%87%D9%88%D8%A7%D8%AA%D9%81_%D8%A7%D9%84%D8%B0%D9%83%D9%8A%D8%A9

21. (خريشة، محمد)، "نصائح لحماية نفسك من الاختراق" موقع تكنواي، عمان، الاردن، يناير
2015

<https://www.technawi.net/%D9%86%D8%B5%D8%A7%D8%A6%D8%AD-%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D9%86%D9%81%D8%B3%D9%83-%D9%85%D9%86-%D8%A7%D9%84%D8%A5%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%A7%D9%84%D8%AC%D8%B2%D8%A1-2/>

الملاحق:

ملحق رقم (1)

بطاقة مقابلة

اليوم: الثلاثاء

التاريخ: 2019/2/19

الساعة: 9:00 ص

الهدف من المقابلة

التعرف إلى المخاطر الأمنية للهواتف الذكية والتي تتعرض لها الطالبات، وأهم السبل والطرق والاحتياطات اللازمة لتجنب تلك المخاطر .

نوع الأسئلة:

أسئلة مفتوحة

العينة المستهدفة:

المقدم: نضال كلاب، مدير الشرطة بمحافظة خان يونس.

صيغة أسئلة المقابلة:

1.حدثنا عن المخاطر الأمنية للتقنيات الرقمية؟ وبرأيك ماهي أكثر تلك المخاطر التي تتعرض لها الفتيات من وجهة نظرك؟

2.برأيك ماهي الطرق والاحتياطات الأمنية التي يمكن أن تقوم بها الفتيات لتقليل تلك المخاطر الى أدنى درجة ممكنة؟

3. أنتم كمؤسسة أمنية وشرطية تابعة لوزارة الداخلية هل كان لكم دور في نشر الوعي الأمني والثقافة الأمنية للتقنيات الرقمية بين المواطنين، وهل ارتقى دوركم الى الدرجة المطلوبة؟

ملحق (2)

استبانة

الأمن الرقمي لدى طالبات المدارس الثانوية في مدينة خان يونس وسبل تعزيزه

عزيزتي الطالبة/

نرجو منك الإجابة عن فقرات الاستبانة بمصادقية وموضوعية، حيث سوف يتم استخدامها بهدف البحث العلمي فقط.

الرقم	الفقرة	درجة	درجة	درجة
		كبيرة	متوسطة	قليلة
1	أستخدم كلمة مرور خاصة بي ومكونة من أكثر من 14 حرف.			
2	أبتعد عن استخدام نفس كلمة المرور على حسابات أخرى.			
3	أتجنب فتح الاعلانات المشبوهة التي عادة ما تكون مرتبطة ببعض التطبيقات.			
4	أقوم باستخدام برنامج مضادة للفيروسات.			
5	أضع لاصقا على الكاميرا أثناء استخدامي لهاتفي.			
6	أتجنب إضافة أي أشخاص على شبكات التواصل الاجتماعي الخاصة بي ان كنت غير متأكدة من هويتهم.			
7	أقوم بإغلاق شبكة الواي فاي مباشرة بعد الانتهاء من حاجتي لها.			
8	أبتعد عن فتح الروابط التي تحوي المعلومات المثيرة.			
9	أتجنب نشر صوري على مواقع التواصل في المناسبات.			

			أبتعد عن ترك هاتفني مع أي شخص غير موثوق به.	10
			أتجنب فتح المرفقات من مصادر غير معروفة.	11

ملحق رقم 3

