

إدمان طفل العصر الرقمي على الانترنت و ضرورة الأمن الإلكتروني

د./مرابية نسيم¹

¹ — جامعة علي لونيبي البلدية 02 (الجزائر)، nassima.merabia73@gmail.com

تاريخ الاستلام: 2024 /03/18 تاريخ القبول: 2023/..../ تاريخ النشر: 2024/06./30

ملخص:

إن ظهور الثورة الصناعية الثالثة و الرابعة نقلتنا إلى عصر تكنولوجيا المعرفة والمعلومات، وعصر البيانات الضخمة، والذكاء الاصطناعي وتطبيقاته مما أحدث نقلة نوعية في حياتنا من خلال مزج الثقافات والعلوم، لنجد أنفسنا أمام عصر ثقافة الحاسب والاتصالات والإنترنت، والذي أصبحنا مطالبين بإتقانه، ومعرفة ما يتبعه من معرفة ومغزى، و ضرورة الأمن الإلكتروني للفئات الأصغر سنا و التي تتراوح ما بين 5-17 سنة وهي الأكثر استعمالا بعد جائحة كورونا فاصح ادماهم عليه له تأثيرات حسب متغيرين نوع الأثر وحسب نوع المؤثر. فكيف يمكن أن نضمن تشكيل ثقافة الكترونية للطفل دون توفير امن إلكتروني؟

ان الهدف من الدراسة الوصفية هو معرفة ما إذا كانت هناك عقلنة في اخضاع الطفل لهذا المحتوى الافتراضي ، من حيث تحديد العناصر تحديد وقت الاستخدام و مدته ، تحديد محتواه ،و تحديد مقدار أضراره من منفعه من طرف الفاعلين التربويين ،و الأولياء هم أول الفاعلين التربويين ،إذ تقع عليهم مسؤولية أمنهم الإلكتروني إذ من الممكن أن تكون كوارث على الطرفين معا الآباء و الأبناء.

الكلمات المفتاحية : الطفل الرقمي ، الإدمان ،الأمن الإلكتروني، البصمة الالكترونية،

Abstract:

The emergence of the third and fourth industrial revolution moved us to the era of knowledge and information technology, the era of big data, artificial intelligence and its applications, which created a qualitative shift in our

lives by blending cultures and sciences, to find ourselves in front of the era of computer culture, communications and the Internet, which we have become required to master it, and to know what follows from knowledge and meaning, and the necessity of electronic security for younger groups that range between 5-17 years, which is the most used after the Corona pandemic, so their addiction to it has effects according to two variables, the type of impact and the type of impact. How can we ensure the formation of an e-culture for children without providing cybersecurity?

The aim of the descriptive study is to find out whether there is rationality in subjecting the child to this virtual content, in terms of determining the elements, determining the time and duration of use, determining its content, and determining the amount of its harms from its benefits by educational actors, and parents are the first educational actors, as they are responsible for their cyber security, as it can be disastrous for both parents and children.

Keywords: Digital child, addiction, cybersecurity, electronic fingerprint,

مقدمة

إن الوسائط الالكترونية تعد من أهم مصادر بناء ثقافة طفل العصر الرقمي والمتمثلة في المواقع الالكترونية ، و الكتاب الالكتروني و الألعاب الالكترونية و البريد الالكتروني ، فبتعدد أبعاد هذه الوسائط تتعدد انعكاساتها في الجوانب الثقافية للطفل، نظرًا لما تحتويه من تأثيرات بصرية وسمعية وحسية المتنوعة، بالإضافة إلى اقتناعهم التام بأن هذه الألعاب توفر لهم التسلية والمرح، ولكن في حقيقة الأمر فهي تتسم بالخطورة القصوى، في حالة الإفراط في استخدامها دون الشروط والضوابط المحددة، فالكثير منها مستوحى من الصراعات والحروب، مما يترك أثرًا نفسيًا وسلوكيًا عدوانيًا سيئًا عند الأطفال والمراهقين. فتدخلهم في دائرة الادمان عليها ، و بعض الانحرافات السلوكية و الأخلاقية¹ (نشوي عبج الغني، دزن سنة، إدمان الانترنت وعلاقته ببعض الاعراض النفسية المرضية لدى طالب المدارس الثانوية . رسالة ماجستير غير منشورة . جامعة حلوان . كلية آداب . قسم علم النفس) التي تختلف مستوياتها و درجة انحرافها حسب نوعية اهتمامات الطفل بهذه المواقع و درجة وعيه والوعي الأسري بها. فبقدر ما تعد هذه الوسائط الالكترونية وسيلة تعليمية توفر النتاج العقلي للطفل الا أنه اذا تزامنت مع متغيرات كالمدة الزمنية التي يقضيها مع هذه الوسائل و

المحتوى الذي يشاهده أو يشاركه مع الآخرين، و مقدار أضرارها علي الطفل ضرار يكون هذا مدعاة الى تساؤلات عدة منها :

- هل يمكن التحكم بمصادر و مجالات استخدام الطفل للوسائط الالكترونية في الوقت الراهن ؟
- هل الطفل الجزائري مكتسب للثقافة الالكترونية بصورة عقلانية؟
- كيف يمكن أن نضمن تشكيل ثقافة الكترونية للطفل دون توفير امن إلكتروني؟

1- هل يجب أن نخاف من تأثير التكنولوجيا على الأطفال؟

في هذا العصر بدأت التكنولوجيا الحديثة وأدواتها تنتشر بين الأيدي الصغيرة بعد أن وصلت لمعظم سكان الكرة الأرضية من البالغين. كما بدأ تأثير التكنولوجيا على ثقافة الأطفال ايجابيا و سلبيا ،لذا فقد أصبح لزاماً علينا أن نعيد النظر فيها بنظرة فاحصة مدققة. (2. هند علي ليلة 4108). الفروق بين نمطي الاستخدام المفرط للإنترنت في إدارة الوقت والبحث الحسي . رسالة ماجستير غير منشورة . جامعة المنيا . كلية التربية . قسم الصحة النفسية)

فهل هي فقط مغارف يستعين بها أطفالنا على الوصول للعلوم والفهم والثقافة والتسلية؟ أم أن آثارها على أطفالنا أصبحت معاول هدم لصحتهم الجسدية والنفسية والاجتماعية؟

يمكن للشاشات والإنترنت ووسائل التواصل الاجتماعي أن تكون أدوات لتطوير المهارات اللغوية و الفكرية و تطوير نشاطاته العقلية إذا كانت هناك عقلنة في اخضاع الطفل لهذا المحتوى الافتراضي ، من حيث تحديد العناصر السابقة الذكر من - تحديد وقت الاستخدام و مدته ، تحديد محتواه ،تحديد مقدار أضراره من منافع من طرف الفاعلين التربويين و الأولياء هم أول الفاعلين التربويين ،إذ تقع عليهم مسؤولية أمنهم الإلكتروني إذ من الممكن أن تكون كوارث على الطرفين معا الآباء و الأبناء .

2- لماذا يدمن الطفل ؟

يدمن عادة بسبب الشعور بالوحدة، أو الفراغ، أو الملل، أو بسبب مشاكل اجتماعية أو أسرية أو مادية يريد أن يتناساها، أو بسبب جو يفرضه الأصدقاء لا ننتبه إلى عواقبه³.

3- . تعريف إدمان الإنترنت والتكنولوجيا

كتعريف فإن الأكثر قبولاً بين العلماء هو الاستخدام المفرط الذي لا يمكن السيطرة عليه للإنترنت مصحوباً بأعراض الانسحاب بحيث يصبح المدمن غير قادرٍ على إدارة حياته بشكل عام وينطوي على الإنترنت بعيداً عن مجتمعه ومحيطه. ومن أبرز أمثلة الإدمان التي يعيشها الكثير من أبنائنا والشباب في هذا العصر هو الإدمان على ألعاب الكمبيوتر والجلوس أمامه لساعات طويلة متواصلة وصعوبة خروجهم من دوامتها.

4- علامات الإدمان

- الشعور بالقلق والتوتر إذا لم يتمكن من اللعب.
- كثرة التفكير بما تم تحقيقه في اللعبة، أو بما سيفعله في المرة القادمة التي سيلعب بها.
- الكذب ومحاولة إخفاء الحقيقة في الوقت الذي يقضيه في ألعاب الفيديو خاصة على الأهل والأصدقاء.
- العزلة والانطوائية وتفضيل اللعب على الحياة الاجتماعية والعائلية⁴.
- فقدان الاهتمام بممارسة الهوايات.
- الإرهاق والتعب العام والصداع.
- ألم متزايد في رسغ وأصابع اليد.
- إهمال الصحة والنظافة الشخصية.

5- تأثيرات الادمان الالكتروني على الطفل :

منذ جائحة الكورونا، فإن الكثير من الآباء وأيضاً الأطفال لجأوا إلى الإنترنت كطوق نجاة للتواصل مع الآخرين واستعادة شكلٍ من أشكال الحياة الاجتماعية التي اعتادوها. وخلالها كان الجميع مضطرين لتقديم بعض التنازلات التنازل عن القوانين الصارمة فيما يتعلق بالجلوس لساعات طويلة على الإنترنت، مثل عدد الساعات. ولكن وخلال هذه الممارسات اليومية فإن عادات ومخاوف أيضاً نشأت حول صحة أبنائهم الجسدية والنفسية. كما نشأت مخاوف أيضاً حول مع من يقضون أوقاتهم على صفحات التواصل الاجتماعي وباقي مواقع الإنترنت. كما نشأت المخاوف أيضاً حول المحتوى والمعارف والعادات التي يكتسبونها.

وقد أشارت دراسة حديثة أن مجموعة متزايدة من الدراسات تذكر أن الإفراط والإدمان للوسائط الرقمية لها آثار وعواقب ضارة جسدية ونفسية واجتماعية وعصبية . كما تشير الدراسات إلى أن المدة والمحتوى والاستخدام في ساعات الليل ونوع الوسائط هي عوامل لها تأثيرها على مستوى الضرر.

5-1- تقسيم تأثير التكنولوجيا على الأطفال حسب نوع الأثر⁵

5-1-1 الآثار النفسية والعقلية المترتبة عن تعامل الأطفال مع التكنولوجيا

لم توجد أدلة على وجود علاقة سببية في الدراسات النفسية على أن لأنشطة التي يديها الأطفال في تعاملهم مع الانترنت إذ ليس بالضرورة وجود مشاكل في الصحة العقلية وبعض الآثار السلبية ،يعني أيضاً أن من لديه مشاكل في الصحة العقلية قد يتأثر بهذه الأسباب أكثر من غيره. كما لوحظ وجود ارتباط بين الذين ينخرطون في الأنشطة القائمة على الشاشة بشكل متكرر أو لفترات أطول بوجود مشاكل في الصحة العقلية، ولكن لم تثبت بعد أن هذه الأنشطة كانت السبب. وهذا لا يعني بانعدام التأثير . ومن هذه الآثار السلبية على الصحة العقلية والنفسية ما يلي:

- القلق
- الاكتئاب
- الإحباط
- الإدمان على الإنترنت بمصاحبة علامات وتختلف درجتها من طفل الى آخر
- ضعف الثقة بالنفس
- الإنسحاب
- الميول الإنتحارية
- اضطراب فرط الحركة ونقص الإنتباه ADHD
- مخاطر بيولوجية عصبية
- مخاطر على سلامة دماغ الطفل

فعلى سبيل المثال، قامت الكثير من الدراسات لتمييز الآثار المترتبة على إدمان الإنترنت. ومن هذه الدراسات ما وثقت آثار المخاطر الشخصية النفسية. ووفقا للدراسات الاحصائية فإن نسبة الإدمان على الإنترنت بين طلاب المدارس عالميا هي 6% تقريباً⁶.

كما ذكرت الدراسات أن التأثيرات النفسية المتعلقة بقلة النوم نتيجة الإفراط في الجلوس أمام الشاشات والاستخدام الليلي للأجهزة الرقمية قد ترتبط بأعراض كالإكتئاب والميول الإنتحارية. وأيضاً فإن اضطراب فرط الحركة ونقص الإنتباه ADHD أيضاً قد تم ربطه بهذه العوامل وأيضاً بعامل المحتوى العنيف وسريع الحركة. والذي قد يتجاوز هذا الإضطراب إلى ممارسة السلوك العدواني وانخفاض السلوك الاجتماعي الإيجابي عند الأطفال والمراهقين.

وقد أجريت دراسة تم عملها عبر التخطيط المقطعي لدماغ الأطفال في مرحلة ما قبل رياض الأطفال لدراسة تأثير أدمغتهم مع استخدام الوسائط المستندة إلى الشاشة. ووجدت هذه الدراسة ارتباطاً بين زيادة استخدام هذه الوسائط، مقارنةً بإرشادات الأكاديمية الأمريكية لطب الأطفال (AAP)، وانخفاض سلامة البنية المجهرية لمسارات المادة البيضاء في الدماغ. هذه المسارات هي بالمناسبة المسؤولة عن دعم تعلم اللغة ومهارات القراءة والكتابة الناشئة لدى الأطفال في هذه المرحلة. كما يشكل هذا الاستخدام مخاطر بيولوجية عصبية عند الأطفال. الأمر الذي أثر على كيفية لعب الأطفال وتعلمهم وتكوين العلاقات

5-1-2- الآثار الجسدية المترتبة عن تعامل الأطفال مع التكنولوجيا

ان جلوس الطفل أمام الشاشة لساعات كثيرة له علاقة بكثير من الآثار السلبية والأضرار على صحة الأشخاص والأطفال بالأخص. ومن هذه الآثار ما يلي:

- قلة النوم وعدم كفايته
- ضعف البصر،
- هشاشة العظام،
- ضعف الجسم،
- مخاطر أمراض القلب والأوعية الدموية مثل:

- ارتفاع ضغط الدم،
- السمنة،
- انخفاض الكوليسترول الحميد،
- تنظيم ضعيف للإجهاد (استثارة عالية الودي وعدم انتظام الكورتيزول
- مقاومة الأنسولين.

5-1-3- تأثير التكنولوجيا على الأطفال في السلوك والتربية والتعليم

سنذكر هنا مجموعة من الآثار السلبية للتكنولوجيا على الأطفال من حيث النواحي السلوكية والتربوية والتعليمية. كما سنمر سريعاً على النتائج السلبية التي ستنتج أيضاً عن تعامل الأطفال غير المنضبط مع التكنولوجيا.

📌 تأثير التكنولوجيا على الأطفال في السلوك العام:

- العدوانية نتيجة ألعاب الكمبيوتر العنيفة. ويظهر أثرها في التنمر الإلكتروني، واللجوء إلى العنف كما حصل في حوادث إطلاق النار في المدارس؛
- ردود الأفعال العنيفة؛
- الوقوع في الاستغلال الجنسي عبر الإنترنت والنتائج عن التعامل مع بالغين عبر الإنترنت ممتنين لهذه المهنة؛
- الانتحار (نتيجة الاندماج في ألعاب تؤثر على عقل الطفل بشكل هدام مثل لعبة الحوت الأزرق).

📌 تأثير التكنولوجيا على الأطفال في التربية:

- السلبية والإعتمادية على الغير؛
- فقدان الخصوصية والأمن نتيجة عدم أخذ الإحتياطات، وبالتالي تعرض الطفل لمختلف أنواع الاستغلال والمحتوى السيئ.
- اكتساب عادات مخالفة لأصول التربية الصحيحة؛

تأثير التكنولوجيا على الأطفال في التعليم:

- الإهمال في الوظائف المدرسية؛
 - ضعف الأداء الدراسي والتحصيل؛
 - تشتت وضعف الانتباه ADD ؛
 - محدودية الإبداع (الناتج عن التلقي السلبي)؛
- توفير الأجهزة المحمولة في الواقع فرصًا للاستخدام التفاعلي بين المستخدمين . فعلى سبيل المثال، يمكن عبرها ممارسة الألعاب أو التقاط الصور، أو التعلم عن بعد. وهذه بدورها توفر فرصًا لممارسة الذاكرة العاملة والتخطيط والتحفيز والتثبيط عند الأطفال، وبالتالي قد تساعد في تحسين الوظائف التنفيذية.

5-1-4- الآثار الاجتماعية المترتبة عن تعامل الأطفال مع التكنولوجيا

كما هو متوقع فإن انعزال الطفل لساعات أمام الشاشات يؤدي ويرتبط بالكثير من الآثار الاجتماعية المترتبة عليه , ليس أقل من هذه الآثار ما في هذه القائمة:

- الضعف العاطفي في فترة الطفولة المبكرة
- الانعزال وضعف العلاقات والمهارات الاجتماعية
- قدرة أضعف على فهم المشاعر للمحيطين به
- الإنطواء
- ضعف القدرة على التعبير عن النفس
- ضعف القدرة على الاختلاط بالمجتمع
- ضعف الترابط الأسري

5-2- تقسيم تأثير التكنولوجيا على الأطفال حسب نوع المؤثر

5-2-1 تأثير التكنولوجيا على الأطفال الناتج عن أنواع المحتوى

أما بالنسبة للمحتوى وعدد ساعات العمل على الإنترنت، فإن الكثير من الأولياء يضعون قواعد صارمة فيما يتعلق بها. ولكن هل للمحتوى التأثير نفسه لعدد ساعات العمل على الإنترنت من حيث التأثيرات السلوكية والإدمان على الإنترنت؟

بين وقت وآخر نسمع في الأخبار عن أطفال يؤذون أنفسهم أو غيرهم بعد مشاهدتهم محتويات أو ممارستهم ألعاباً عنيفة على الشاشات أو من خلال الإنترنت. ورغم فرض الكثير من الدول القوانين الشديدة على مزودي خدمات مواقع الإنترنت مثل الفيسبوك وتويتر وغيرها لعدم إتاحة هكذا محتوى للأطفال والعامة، إلا أنه لم يتحقق الكثير من التقدم رغم ذلك Social media, screen time, and young people's mental health, [Social media, screen time, and young people's mental health - The Lancet, Volume 393, Issue 10172](#) p611 February 16, 2019)

5-2-2 تأثير التكنولوجيا على الأطفال الناتج عن الوقت أمام الشاشة :

بالنسبة للآباء والمعلمين والأطباء، “وقت الشاشة” هو مصطلح محمل وقد يعكس عددًا من التعريفات المختلفة للآباء والباحثين. إن التقدم التكنولوجي والتوافر المتزايد لتقنيات الهاتف المحمول يفوقان بكثير الأبحاث، مما يجعل من الصعب معرفة ما هو “المناسب” للأطفال، لا سيما في عصر يتم فيه استخدام الشاشات بشكل متزايد للأغراض التعليمية.

6- كيفية تجنب معظم أنواع الجرائم الإلكترونية :

أن ما يترتب على ادمان الطفل للانترنت عواقب وخيمة منها التعرض الى للجرائم الإلكترونية و لتجنب ذلك نتبع التدابير التالية :

عدم فتح الروابط في رسائل البريد الإلكتروني العشوائية أو على مواقع الويب غير الموثوق بها. كما توجد طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونية، وهي فتح الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو الرسائل الأخرى أو المواقع الإلكترونية غير المألوفة.

لتجنّب القيام بهذا الأمر للحفاظ على أمنك و أمن الطفل على الإنترنت. فيتوقف ذلك على ترقية الآباء علاقتهم التكنولوجية مع وسائل الاتصال الحديثة لمعرفة كيفية التعامل معها ،و تكييف محتوياتها ليكونوا أمنا لأبنائهم و تدريبهم على الامن الالكتروني بدورهم .⁷

7- المقصود بالأمن الإلكتروني و ضرورة أمن الطفل الكترونيا.

7-1- ما المقصود بالأمن الإلكتروني؟⁸

الأمن الإلكتروني هو حماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة. ويُعرف أيضًا بأمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية. وهذا المصطلح مستخدم في سياقات مختلفة من الأعمال إلى الحوسبة المتنقلة، ويمكن تقسيمه إلى عدة فئات شائعة.

- **أمن الشبكات** هو ممارسات حماية شبكة الحاسوب من المتسللين، سواء كانوا من المهاجمين الذين يستهدفون الشبكة أو من البرامج الضارة الباحثة عن أي ثغرة تستغلها.
- **أمن التطبيقات** يركّز على إبقاء البرامج والأجهزة بمنأى عن التهديدات، واختراق أي تطبيق قد يتسبب في الوصول إلى البيانات التي تم تصميم التطبيق لحمايتها. ويبدأ الأمن الناجح في مرحلة التصميم، أي قبل فترة طويلة من نشر البرنامج أو الجهاز.
- **أمن المعلومات** يحمي سلامة البيانات وخصوصيتها عندما تكون مخزنة وأثناء نقلها على حدٍ سواء.
- **أمن العمليات** يتضمن العمليات والقرارات التي تتعلق بمعالجة أصول البيانات وحمايتها. تشمل هذه الفئة الأذونات التي يملكها المستخدمون عند الوصول إلى شبكة معينة والعمليات التي تحدد كيفية تخزين البيانات أو مشاركتها ومكان ذلك.
- **التعافي من الكوارث واستمرارية الأعمال** تحدد كيفية استجابة مؤسسة ما لحادث أمن إلكتروني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات. سياسات التعافي من الكوارث تحدد كيفية استرداد المؤسسات لعملياتها ومعلوماتها لاستعادة القدرة التشغيلية نفسها التي كانت عليها قبل الحدث، أما استمرارية الأعمال فهي الخطة التي تستند إليها المؤسسة عند محاولتها العمل من دون موارد معينة.
- **تعليم المستخدم النهائي** هي الفئة التي تتعامل مع أكثر عامل غير متوقّع للأمن الإلكتروني، ألا وهو الأشخاص. يمكن أن يُدخل أي شخص عن غير قصد فيروسًا إلى نظام آمن نتيجة عدم اتباع الممارسات

الأمنية الجيدة. وبالتالي، تعليم المستخدمين كيفية حذف مرفقات البريد الإلكتروني المريبة وعدم توصيل محركات أقراص USB مجهولة المصدر وتلقيهم دروساً متنوعة أمر مهم وأساسي لأمن أي مؤسسة.

7-2- حجم التهديد الإلكتروني

التهديدات الإلكترونية العالمية تتطور بوتيرة سريعة، ويترافق ذلك مع ارتفاع في عدد انتهاكات البيانات كل عام. أظهر تقرير صادر عن شركة RiskBased Security أن عددًا كبيرًا يبلغ 7,9 مليار سجلًا قد تعرّضوا لاختراقات بيانات خلال الأشهر التسعة الأولى من عام 2019 وحده. يفوق هذا الرقم ضعف (112%) عدد السجلات التي تعرّضت لاختراقات خلال الفترة نفسها من عام 2018.

وقد شهدت الخدمات الطبية ومتاجر البيع بالتجزئة والكيانات العامة العدد الأكبر من الاختراقات، وكانت الهجمات الخبيثة وراء معظم هذه الحوادث. تجذب بعض هذه القطاعات المجرمين الإلكترونيين أكثر من غيرها بسبب جمعهم للبيانات المالية والطبية، غير أنه من الممكن أن تكون كل الشركات التي تستخدم الشبكات هدفًا للحصول على بيانات العملاء أو للتجسس على الشركة أو للهجمات على العملاء.

ومع توقُّع تزايد حجم التهديد الإلكتروني، تتوقَّع مؤسسة International Data Corporation أن يبلغ الإنفاق العالمي على حلول الأمن الإلكتروني 133,7 مليار دولارًا أمريكيًا بحلول عام 2022. واستجابت الحكومات في جميع أنحاء العالم للتهديد الإلكتروني المتزايد بتقديم إرشادات لمساعدة المؤسسات على تطبيق ممارسات أمن إلكتروني فعالة.

ففي الولايات المتحدة، وضع المعهد الوطني للمعايير والتكنولوجيا (NIST) إطار الأمن الإلكتروني. ولحاربة انتشار البرمجيات الخبيثة والمساعدة في الاكتشاف المبكر للهجمات، ينصح الإطار بمراقبة كل الموارد الإلكترونية بشكل متواصل وفوري. وتم ذكر مدى أهمية مراقبة الأنظمة في الإرشادات المعنونة "10" "steps to cyber security" (خطوات العشر لتعزيز الأمن الإلكتروني) التي قدّمها المركز القومي للأمن الإلكتروني التابع لحكومة المملكة المتحدة. وفي أستراليا، ينشر مركز الأمن الإلكتروني الأسترالي (ACSC) بانتظام إرشادات حول كيفية مواجهة المؤسسات أحدث التهديدات في مجال الأمن الإلكتروني.

7-3- أنواع التهديدات الإلكترونية

تأتي تهديدات الأمن الإلكتروني في ثلاثة أشكال:

1. الجريمة الإلكترونية التي تتضمن جهات فاعلة فردية أو مجموعات تستهدف الأنظمة لاكتساب ربح مالي أو للتسبب بعطل.
 2. الهجوم الإلكتروني الذي غالبًا ما يتضمن جمع المعلومات بدوافع سياسية.
 3. الإرهاب الإلكتروني الذي يهدف إلى إضعاف الأنظمة الإلكترونية من أجل التسبب بحالة هلع أو خوف.
- إذًا، كيف تتحكم الجهات الفاعلة الضارة في أنظمة أجهزة الكمبيوتر؟ فيما يلي بعض الطرق الشائعة المستخدمة لتهديد الأمن الإلكتروني:

✓ البرامج الضارة

البرامج الضارة تعني البرمجيات الخبيثة، وتشكّل هذه البرامج أحد أكثر التهديدات الإلكترونية شيوعًا، وهي عبارة عن برامج يقوم مجرم إلكتروني أو مخترق بإنشائها لتعطيل جهاز كمبيوتر المستخدم الشرعي أو إلحاق الضرر به. ويمكن للبرامج الضارة، التي غالبًا ما تنتشر عبر مرفق بريد إلكتروني مجهول أو تنزيل يبدو في الظاهر شرعيًا، أن تكون مستخدمة من قبل المجرمين الإلكترونيين لاكتساب المال أو للقيام بهجمات إلكترونية بدوافع سياسية.

يوجد عدد من أنواع البرامج الضارة المختلفة، وتشمل:

- **الفيروسات:** هو برنامج ينسخ نفسه ويُرفقها بملف نظيف وينتشر عبر نظام الكمبيوتر ليصيب الملفات ببرنامج ضار.
- **أحصنة طروادة:** هي نوع من البرامج الضارة التي تتنكر في صورة برنامج شرعي. يخدع المجرمون الإلكترونيون المستخدمين ليقوموا بتحميل أحصنة طروادة على أجهزة الكمبيوتر الخاصة بهم حتى يمكنهم إلحاق الضرر بالبيانات أو جمعها.

- **برامج التجسس:** هو برنامج يسجل سرًا ما يقوم به المستخدم لكي يتمكن المجرمون الإلكترونيون من الاستفادة من هذه المعلومات. على سبيل المثال: يمكن لبرنامج التجسس معرفة تفاصيل بطاقات الائتمان.
- **برامج طلب الفدية:** هي برمجية ضارة تقفل ملفات المستخدم وبياناته مهددةً بمسحها ما لم يتم دفع فدية.
- **الإعلانات المدعومة:** هي برامج إعلانات يمكن استخدامها لنشر البرامج الضارة.
- **شبكات البوت نت:** هي شبكات من أجهزة الكمبيوتر المصابة ببرامج ضارة يستخدمها المجرمون الإلكترونيون لإجراء مهام على الإنترنت من دون إذن المستخدم.
- **حقن إس كيو إل حقن إس كيو إل (تعليمات الاستعلامات البنوية)** هو نوع من الهجوم الإلكتروني المستخدم للتحكم في البيانات وسرقتها من قاعدة بيانات. يستغل المجرمون الإلكترونيون الثغرات الأمنية في التطبيقات المستندة إلى البيانات لإدخال برمجية ضارة إلى قاعدة بيانات عبر نص إس كيو إل ضار، مما يتيح لهم الوصول إلى المعلومات الحساسة في قاعدة البيانات.
- **التصيد الاحتيالي**

التصيد الاحتيالي هو عملية يقوم من خلالها المجرمون الإلكترونيون باستهداف الضحايا عبر إرسال رسائل بريد إلكتروني تبدو وكأنها مرسله من شركة شرعية للحصول على معلومات حساسة. غالبًا ما يتم استخدام هجمات التصيد الاحتيالي لخداع الأشخاص والحصول منهم على بيانات بطاقات الائتمان ومعلومات شخصية أخرى.

▪ هجوم الوسيط

إن هجوم الوسيط هو نوع من التهديد الإلكتروني يقوم من خلاله مجرم إلكتروني بمقاطعة الاتصالات بين شخصين بهدف سرقة البيانات. على سبيل المثال: قد يقطع مهاجم البيانات التي يتم تمريرها على شبكة واي فاي غير آمنة من جهاز الضحية إلى الشبكة.

■ هجوم حجب الخدمة

من خلال هجوم حجب الخدمة، يمنع المجرمون الإلكترونيون نظام الكمبيوتر من تنفيذ الطلبات المشروعة عن طريق زيادة حركة البيانات بشكل مفرط على الشبكات والخوادم. بذلك، يصبح النظام غير صالح للاستخدام، مما يمنع المؤسسة من تنفيذ الوظائف المهمة.

7-4- أحدث التهديدات الإلكترونية

ما هي أحدث التهديدات الإلكترونية التي يحتاج الأفراد والمؤسسات إلى حماية أنفسهم منها؟ في ما يلي بعض من أحدث التهديدات الإلكترونية التي بلغت عنها الحكومات البريطانية والأمريكية والأسترالية.

- البرنامج الضار "دريدكس (Dridex)"

في ديسمبر عام 2019، أصدرت وزارة العدل الأمريكية حكمًا على قائد مجموعة من المجرمين الإلكترونيين لدوره في إطلاق هجوم البرنامج الضار "دريدكس" العالمي. ألحقت هذه الحملة الضارة الضرر بالشعب والحكومة والبنية التحتية والشركات حول العالم.

إن "دريدكس" هو حصان طروادة مالي يتمتع بمجموعة من القدرات. ومنذ عام 2014 فإنه يلحق الضرر بالضحايا ويستهدف أجهزة الكمبيوتر من خلال رسائل التصيد الاحتيالي عبر البريد الإلكتروني أو البرامج الضارة القائمة. بقدرته على سرقة كلمات المرور وتفاصيل الحسابات المصرفية والبيانات الشخصية التي يمكن استخدامها في معاملات احتيالية قد تسبب في خسائر مالية هائلة تصل قيمتها إلى مئات الملايين.

ردًا على هجمات دريدكس، قدّم المركز القومي للأمن الإلكتروني التابع لحكومة المملكة المتحدة نصيحة للشعب تقضي "بالحرص على إصلاح أخطاء الأجهزة وتشغيل برنامج مكافحة الفيروسات وتحديثه وإنشاء نسخ احتياطية للملفات".

- الحيل الرومانسية

وفي فبراير عام 2020، حذر مكتب التحقيقات الفيدرالي المواطنين الأمريكيين من خدعة الثقة التي يقوم بها المجرمون الإلكترونيون عبر استخدام مواقع المواعدة وغرف الدردشة وتطبيقاتها، إذ يستغل الجناة الأشخاص الذين يبحثون عن شركاء جدد، ويخدعون الضحايا للحصول منهم على بيانات شخصية.

تظهر تقارير مكتب التحقيقات الفيدرالي أن التهديدات الإلكترونية الرومانسية ألحقت الضرر بما يصل إلى 114 ضحية في نيو مكسيكو عام 2019، كما تسببت بخسائر مالية بلغت 1,6 مليون دولار أمريكي.

البرنامج الضار "إيموتيت (Emotet)"

في أواخر عام 2019، حذر مركز الأمن الإلكتروني الأسترالي المؤسسات الوطنية من تهديد إلكتروني منتشر عالميًا مصدره البرنامج الضار "إيموتيت".

إن إيموتيت عبارة عن حصان طروادة معقد يمكنه سرقة البيانات وتحميل برامج ضارة أخرى. يستفيد "إيموتيت" من كلمات المرور غير المعقدة لتحقيق هدفه: وهذا تذكير بمدى أهمية إنشاء كلمة مرور قوية لتوفير الحماية من التهديدات الإلكترونية.

7-5- حماية المستخدم النهائي

إن حماية المستخدم النهائي أو أمن نقطة النهاية جزء أساسي من الأمن الإلكتروني. في النهاية، غالبًا ما يكون فرد (المستخدم النهائي) هو من يحمل البرامج الضارة أو شكل آخر من أشكال التهديد الإلكتروني على جهاز الكمبيوتر المكتبي أو جهاز الكمبيوتر المحمول أو الجهاز المحمول الخاص به.

إذًا، كيف تحمي تدابير الأمن الإلكتروني المستخدمين النهائيين والأنظمة؟ أولاً: يعتمد الأمن الإلكتروني على بروتوكولات مشفرة لتشفير رسائل البريد الإلكتروني والملفات والبيانات المهمة الأخرى. لا يحمي ذلك المعلومات أثناء نقلها فحسب، بل يحميها أيضًا من فقدانها أو سرقتها.

بالإضافة إلى ذلك، تقوم برامج الأمن الخاصة بالمستخدم النهائي بفحص أجهزة الكمبيوتر بحثًا عن أي برمجيات ضارة وعزلها ثم تزيلها من على الجهاز. بإمكان برامج الأمن أن تكتشف حتى البرمجيات الضارة

المختبئة في سجل التشغيل الرئيسي (MBR) وتزيلها، وهي مصممة لتشفير البيانات أو مسحها من محرك الأقراص الثابتة الخاص بجهاز الكمبيوتر.

وتركز أيضًا بروتوكولات الأمن الإلكتروني على اكتشاف البرامج الضارة بشكل فوري. يستخدم الكثير من هذه البروتوكولات التحليل التجريبي والسلوكي لمراقبة سلوك برنامج وعمله لتوفير الحماية من الفيروسات أو أحصنة طروادة التي تغير شكلها مع كل عملية تنفيذ (البرامج المتعددة الأشكال أو المتحوّلة). يمكن أن تحجز برامج الأمن البرامج التي من المحتمل أن تكون ضارة في فقاعة افتراضية منفصلة عن شبكة المستخدم لتحليل سلوكها ومعرفة كيفية تحسين عملية اكتشاف الإصابات الجديدة.

تحصل برامج الأمن على تطورات دفاعية جديدة حيث يعمل الخبراء في مجال الأمن الإلكتروني على تحديد التهديدات الجديدة وطرق محاربتها. للاستفادة إلى أقصى حد من برامج الأمن الخاصة بالمستخدم النهائي، من الضروري أن يتعلم الموظفون كيفية استخدامها. والأهم هو أن الاستمرار بتشغيلها وتحديثها بشكل منتظم يضمن قدرتها على حماية المستخدمين من أحدث التهديدات الإلكترونية.

6-7- نصائح الأمن الإلكتروني - حماية نفسك من الهجمات الإلكترونية

كيف يمكن للشركات والأفراد حماية أنفسهم من التهديدات الإلكترونية؟ إليك مجموعة من أهم نصائح الأمن الإلكتروني:

- تحديث التطبيقات ونظام التشغيل: يعني هذا الاستفادة من أحدث التصحيحات الأمنية.
- استخدام برامج مكافحة الفيروسات: حلول الأمن مثل Kaspersky Total Security ستكتشف التهديدات وتزيلها. أبق برنامجك محدثًا للحصول على أفضل مستوى من الحماية.
- استخدام كلمات مرور قوية: احرص على ألا تكون كلمات المرور الخاصة بك سهلة التخمين.
- لا تفتح مرفقات البريد الإلكتروني من المرسلين الذين لا تعرفهم: قد تكون مصابة ببرامج ضارة.
- لا تفتح أي روابط في رسائل البريد الإلكتروني المرسلة من مرسلين لا تعرفهم أو على مواقع إلكترونية غير معروفة: هذه طريقة شائعة لنشر البرامج الضارة.

■ **تجنب استخدام شبكات WiFi غير آمنة في الأماكن العامة:** تعرضك الشبكات غير الآمنة لخطر الهجمات الوسيط.

■ **بهدف حماية المستخدمين.. ميتا تبدأ تشفير رسائل فيسبوك وماسنجر**

ديسمبر 2023 ستتيح الخاصية الجديدة تشفير الرسائل بشكل تلقائي على فيسبوك وماسنجر - رويترز و أكدت ميتا أن خاصية التشفير التام ستكون متاحة على الفور لجميع المحادثات والمكالمات الشخصية على ماسنجر وفيسبوك لحماية المستخدمين من عمليات القرصنة.

أعلنت شركة "ميتا بلااتفورمز" أنها بدأت التشفير التام لجميع المحادثات والمكالمات الشخصية على ماسنجر وفيسبوك. وأوضحت ميتا أن برنامج ماسنجر كان لديه في السابق خيار تشغيل خاصية التشفير التام مما يسمح بقراءة الرسائل من قبل المرسل والمتلقي فقط، ولكن مع هذا التغيير سيتم تشفير الرسائل بشكل تلقائي⁹. "ميتا" تدفع نحو تعزيز الخصوصية كما يدرس تطبيق واتساب احتمال إضافة ميزة اسم مستخدم إلى الملف الشخصي، على غرار الأسماء الخاصة بالمستخدمين في مواقع التواصل الاجتماعي كإنستغرام وتويتر، وذلك لمنح المزيد من الخصوصية للمستخدمين عبر تمكينهم من إخفاء رقم هاتفهم خلال المحادثات الفردية والجماعية <https://www.skynewsarabia.com/business/1676021>.

وكانت شركة "ميتا" قد أعلنت في يونيو/ حزيران الماضي عن إجراءات وقائية وقيود لضبط المحتوى المقدم لفئة المراهقين والأطفال. وتتضمن الإجراءات ضوابط على تطبيق ماسنجر، تتيح للوالدين الإشراف على تطبيق المراسلة الفورية.

8- كيف نحمي بصمتنا الالكترونية من المتسللين :

كيف تحمي أجهزتك و شبكتك المنزلية من مخاطر التعرض للهجمات السبرانية التي تكلفنا خسائر مالية أو تنتهك خصوصيتنا أو قد يتعرض طفلك الى احدى الجرائم البرانية من تحرش او ابتزاز أو تصيد الكتروني عبر مواقع او روابط لا يعي الطفل كيف دخل فيها و كيف تورط في مثل هذه الجرائم .

يوصي التقنيون في التكنولوجيا¹⁰ بحملة من التوصيات كوقاية من هذه الجرائم و الهجمات منها ما يلي :

ضع كلمة سر قوية على أجهزة الشبكة

غير الاعدادات الافتراضية لأجهزة الشبكة

كن على علم دائم بالأجهزة المتصلة لشبكتك

✚ فعل خاصية التشفير الموجودة في أجهزة الشبكة

✚ حدث الانظمة و البرامج بصفة مستمرة

✚ فعل خاصية التحقق الثنائي للبرامج و التطبيقات

✚ استخدم برامج حماية من الفيروسات و حدثها باستمرار.

لكن ما معنى البصمة الالكترونية أو الرقمية وكيف يكون الفرد المستخدم نشطا أم غير نشط :

ما المقصود بالبصمة الرقمية؟

8-1- البصمة الرقمية - المعنى والتعريف

يشير مصطلح "البصمة الرقمية"، والتي تُسمى أحياناً الظل الرقمي أو البصمة الإلكترونية، إلى أثر البيانات التي تتركها عند استخدام الإنترنت. وهي تشمل مواقع الويب التي تزورها، ورسائل البريد الإلكتروني التي ترسلها، والمعلومات التي تقدمها عبر الإنترنت. يمكن استخدام البصمة الرقمية لتتبع أنشطة أي شخص على الإنترنت وأجهزته. ينشئ مستخدمو الإنترنت بصمتهم الرقمية إما بشكل نشط أو بشكل غير نشط.

8-2- ما المقصود بالبصمة الرقمية؟

أنت تترك وراءك أثراً للمعلومات التي تُعرف باسم البصمة الرقمية الخاصة بك، وذلك عندما تستخدم الإنترنت.¹¹ تنمو البصمة الرقمية بعدة طرق، منها، على سبيل المثال، النشر على وسائل التواصل الاجتماعي أو الاشتراك في رسالة إخبارية أو ترك مراجعة على الإنترنت أو التسوق عبر الإنترنت.

في بعض الأحيان، لا يكون من الواضح دائماً أنك تسهم في بصمتك الرقمية. على سبيل المثال، يمكن لمواقع الويب تتبع نشاطك عن طريق تثبيت ملفات تعريف الارتباط على جهازك، ويمكن للتطبيقات تجميع بياناتك من دون علمك بذلك. وبمجرد أن تسمح لمؤسسة ما بالوصول إلى معلوماتك، يمكنها بيع بياناتك إلى جهات خارجية أو مشاركتها معها. والأسوأ من ذلك أنه قد يتم كشف سرية معلوماتك الشخصية في إطار انتهاك بيانات.

غالبًا ما تسمع المصطلحين "نشط" و"غير نشط" في ما يتعلق بالبصمات الرقمية:

✓ البصمات الرقمية النشطة

البصمة الرقمية النشطة هي حين يشارك المستخدم معلومات عن نفسه عن تعمد، على سبيل المثال من خلال النشر أو المشاركة على مواقع شبكات التواصل الاجتماعي أو المنتديات عبر الإنترنت. إذا قام مستخدم بتسجيل الدخول إلى موقع ويب باسم مستخدم أو ملف تعريف مسجل، فإن أي منشورات يقوم بنشرها تشكل جزءاً من بصمته الرقمية النشطة. تشمل الأنشطة الأخرى التي تسهم في تكوين البصمة الرقمية النشطة ملء نموذج عبر الإنترنت، مثل الاشتراك في رسالة إخبارية أو الموافقة على قبول ملفات تعريف الارتباط في متصفحك.

✓ البصمات الرقمية غير النشطة

يتم إنشاء البصمة الرقمية غير النشطة عندما يتم جمع معلومات حول المستخدم دون أن يدرك أن هذا يحدث. على سبيل المثال، يحدث هذا عندما تجمع مواقع الويب معلومات حول عدد مرات زيارة المستخدم لها، والموقع الذي يدخل منه، وعنوان IP الخاص به. وهذه عملية خفية قد لا يدرك المستخدمون حدوثها. من الأمثلة الأخرى للبصمات غير النشطة مواقع شبكات التواصل الاجتماعي والمعلنين الذين يستخدمون عمليات إبداء الإعجاب والمشاركة والتعليقات لإنشاء ملفك الشخصي واستهدافك بمحتوى محدد.

✓ لماذا تحظى البصمات الرقمية بالأهمية؟

تحظى البصمات الرقمية بالأهمية للأسباب التالية:

- إنها بيانات دائمة نسبياً، وبمجرد أن تصبح متاحة للاطلاع العام أو حتى العام جزئياً، كما هو الحال مع منشورات Facebook، تصبح سيطرة المالك على كيفية استخدام الآخرين لها طفيفة.
- يمكن للبصمة الرقمية أن تحدد السمعة الرقمية للشخص، والتي تضارع في أهميتها الآن مقدار أهمية سمعته على أرض الواقع.
- فبمقدور جهات العمل التحقق من البصمات الرقمية لموظفيهم المحتملين، وخاصة وسائل التواصل الاجتماعي الخاصة بهم، قبل اتخاذ قرارات التوظيف. ويمكن للكليات والجامعات التحقق من البصمات الرقمية لطلابها المحتملين قبل قبولهم أيضاً.

- وقد يمكن إساءة تفسير الكلمات والصور التي تنشرها عبر الإنترنت أو تغييرها، ما يتسبب في إهانة غير مقصودة.
 - ويمكن للمحتوى المخصص لمجموعة خاصة أن ينتشر إلى دائرة أوسع، ما قد يضر بالعلاقات والصدقات.
 - ويمكن لمجرمي الإنترنت استغلال بصمتك الرقمية باستخدامها لأغراض مثل الانتحال للوصول إلى الحساب أو إنشاء هويات مزيفة بناءً على بياناتك .
- لهذه الأسباب، يجدر التفكير مليًا في ما تقوله بصمتك الرقمية عنك. يحاول العديد من الأشخاص إدارة بصمتهم الرقمية من خلال توخي الحذر بشأن أنشطتهم عبر الإنترنت للتحكم في البيانات التي يمكن جمعها عنهم في المقام الأول .

✓ أمثلة على البصمة الرقمية

يمكن أن تكون لدى مستخدم الإنترنت مئات العناصر التي تشكل جزءًا من بصمته الرقمية. ومن بين الطرق التي يضيف بها المستخدمون إلى بصمتهم الرقمية ما يلي:

التسوق عبر الإنترنت

- إجراء عمليات شراء من مواقع التجارة الإلكترونية
- التسجيل للحصول على القسائم أو إنشاء حساب
- تنزيل تطبيقات التسوق واستخدامها
- التسجيل من أجل النشرات الإخبارية للعلامة التجارية

الخدمات البنكية عبر الإنترنت

- استخدام تطبيق الخدمات المصرفية للهاتف المحمول
- بيع الأسهم وشراؤها

- الاشتراك في المطبوعات والمدونات المالية

- فتح حساب بطاقة ائتمان

وسائل التواصل الاجتماعي

- استخدام وسائل التواصل الاجتماعي على جهاز الكمبيوتر أو الأجهزة الخاصة بك

- تسجيل الدخول إلى مواقع الويب الأخرى باستخدام بيانات اعتماد وسائل التواصل الاجتماعي

- التواصل مع الأصدقاء وجهات الاتصال

- مشاركة المعلومات والبيانات والصور مع معارفك

- الانضمام إلى موقع أو تطبيق للمواعدة

قراءة الأخبار

- الاشتراك في مصدر إخباري عبر الإنترنت

- استعراض المقالات على تطبيق إخباري

- التسجيل للاشتراك في النشرة الإخبارية لمطبوعة معينة

- إعادة نشر المقالات والمعلومات التي تقرأها

الصحة واللياقة البدنية

- استخدام أجهزة تتبع اللياقة البدنية

- استخدام التطبيقات لتلقي الرعاية الصحية

- تسجيل عنوان بريدك الإلكتروني لدى صالة ألعاب رياضية

- الاشتراك في مدونات الصحة واللياقة البدنية

✓ حماية بصمتك الرقمية

من الجيد أن تضع بصمتك الرقمية في الحسبان نظرًا إلى أن جهات العمل والكليات وغيرها يمكنها البحث عن هويتك عبر الإنترنت. في ما يلي بعض النصائح لحماية بياناتك الشخصية وإدارة سمعتك عبر الإنترنت.

- استخدام محركات البحث للتحقق من بصمتك الرقمية

أدخل اسمك في محركات البحث. قم بتضمين اسمك الأول والأخير وأي اختلافات في الهجاء. إذا قمت بتغيير اسمك، فابحث عن الأسماء الحالية والسابقة. ستمنحك مراجعة نتائج محرك البحث فكرة عن المعلومات المتاحة عنك للاطلاع العام. إذا كانت أي من النتائج تُظهر كمظهر سلبي، يمكنك الاتصال بمسؤول الموقع لمعرفة ما إذا كان بإمكانه إزالتها أم لا. يعد إعداد تنبيهات Google إحدى الطرق لمراقبة اسمك.

- تقليل عدد مصادر المعلومات التي تذكرك

على سبيل المثال، قد تحتوي مواقع الويب العقارية و whitepages.com على معلومات أكثر مما قد ترغب عنك. غالبًا ما تتضمن هذه المواقع معلومات شخصية، مثل رقم هاتفك وعنوانك وعمرك. إذا لم تشعر بالرضا تجاه ذلك، يمكنك الاتصال بالمواقع الإلكترونية المذكورة وطلب إزالة المعلومات.

- تقييد كمية البيانات التي تشاركها

أنت تقوم بتوسيع بصمتك الرقمية في كل مرة تقدم فيها معلوماتك الشخصية لمؤسسة ما. كما أنك تزيد من احتمالية قيام إحدى المؤسسات التي تخزن بياناتك بإساءة استخدامها أو تعرضها للانتهاك، ما يضع بياناتك بين الأيدي الخطأ. وبناءً على ذلك، ضع في اعتبارك ما إذا كان الأمر يستحق قبل تقديم هذه الاستمارة. هل هناك طرق أخرى للحصول على تلك المعلومات أو الخدمة دون مشاركة بياناتك؟

- التحقق مرة أخرى من إعدادات الخصوصية الخاصة بك

تسمح لك إعدادات الخصوصية على وسائل التواصل الاجتماعي بالتحكم في من يرى منشوراتك. راجع هذه الإعدادات وتأكد من ضبطها على المستوى الذي يناسبك. على سبيل المثال، يتيح لك

Facebook قصر المشاركات على الأصدقاء وإنشاء قوائم مخصصة بالأشخاص الذين يمكنهم مشاهدة منشورات معينة. لكن ضع في اعتبارك أن إعدادات الخصوصية تحمي فقط على موقع وسائل التواصل الاجتماعي ذي الصلة.

- تجنب الإفراط في المشاركة على وسائل التواصل الاجتماعي

تسهل وسائل التواصل الاجتماعي الاتصال بالآخرين ولكن يمكنها أيضًا أن تسهل الإفراط في المشاركة. فكر مليًا قبل الكشف عن موقعك أو خطط السفر أو أي معلوماتك الشخصية الأخرى. تجنب الإفصاح عن رقم هاتفك أو عنوان بريدك الإلكتروني في سيرتك الذاتية على وسائل التواصل الاجتماعي. إنها لفكرة جيدة أيضًا أن تتجنب "إبداء الإعجاب" بالبنك الذي أنت عميل لديه أو مقدم الرعاية الصحية أو الصيدلية التي تتعامل معها وما إلى ذلك؛ لأن هذا قد يقود مجرمي الإنترنت إلى حساباتك المهمة.

- تجنب المواقع غير الآمنة

تأكد من أنك تتعامل مع موقع ويب آمن - يجب أن يبدأ عنوان URL بـ <https://> وليس <http://> - يشير حرف "s" إلى اللفظ "آمن"، ما يشير إلى أن الموقع يحتوي على شهادة أمنية. ويجب أن يكون هناك أيضًا رمز قفل على يسار شريط العنوان. لا تشارك أبدًا أي معلومات سرية على مواقع غير آمنة، وخاصة تفاصيل الدفع.

- تجنب الكشف عن البيانات الخاصة على شبكة Wi-Fi عامة

تعد شبكة Wi-Fi العامة بطبيعتها أقل أمانًا من الشبكة الشخصية لأنك لا تعرف من قام بإعدادها أو من أيضًا قد يشاهدها. تجنب إرسال معلومات شخصية عند استخدام شبكات Wi-Fi عامة.

- حذف الحسابات القديمة

تتمثل إحدى طرق تقليل بصمتك الرقمية في حذف الحسابات القديمة، ومن ذلك، على سبيل المثال، الملفات الشخصية في وسائل التواصل الاجتماعي التي لم تعد تستخدمها أو اشتراكات الرسائل الإخبارية التي لم تعد تقرأها. يقلل التخلص من الحسابات غير النشطة من تعرضك لانتهاكات البيانات المحتملة.

- إنشاء كلمات مرور قوية واستخدام Password Manager

ستساعدك كلمة المرور القوية على الحفاظ على أمنك على الإنترنت. يجب أن تكون كلمة المرور القوية طويلة، أي تتكون من 12 حرفاً على الأقل والأفضل أن تكون أكثر من ذلك، وتحتوي على مزيج من الأحرف الكبيرة والصغيرة، بالإضافة إلى الرموز والأرقام. كلما كانت كلمة مرورك أكثر تعقيداً وصعوبةً، أصبح اختراقها أصعب. سيساعد استخدام Password Manager على إنشاء جميع كلمات المرور الخاصة بك وتخزينها وإدارتها في حساب عبر الإنترنت واحد آمن. حافظ على خصوصية كلمات مرورك عن طريق تجنب مشاركتها مع الآخرين أو كتابتها لهم. حاول تجنب استخدام كلمة المرور نفسها لجميع حساباتك وتذكر أن تغييرها بانتظام.

- مراقبة سجلاتك الطبية

تدرب على الممارسات الجيدة لسلامة أمن البيانات من خلال مراجعة سجلاتك الطبية بشكل دوري. يستهدف لصوص الهوية المعلومات الطبية والصحية وكذلك البيانات المالية. عندما يستخدم المجرمون معلوماتك الشخصية للحصول على علاج طبي باسمك، يمكن أن تتشابك سجلاتك الصحية مع سجلاتك.

- عدم تسجيل الدخول باستخدام Facebook

يعد تسجيل الدخول إلى مواقع الويب والتطبيقات باستخدام Facebook أمراً سهلاً. لكنك، في كل مرة تقوم فيها بتسجيل الدخول إلى موقع ويب تابع لجهة خارجية باستخدام بيانات اعتماد Facebook الخاصة بك، تمنح هذه الشركة الإذن لتعدين بيانات المستخدم الخاصة بك على Facebook ، ما قد يعرض معلوماتك الشخصية للخطر.

- احرص دائماً على تحديث البرنامج

يمكن أن تحتوي البرامج القديمة على ثروة من البصمات الرقمية. ومن دون آخر التحديثات، يمكن لمجرمي الإنترنت الوصول إلى هذه المعلومات. فمجرمو الإنترنت قادرون على الوصول بسهولة إلى أجهزة وبيانات الضحية من خلال استغلال الثغرات في البرامج. ويمكنك المساعدة على منع ذلك عن طريق تحديث برنامجك باستمرار. قد تكون البرامج الأقدم أكثر عرضة لهجمات المتسللين.

- مراجعة استخدام هاتفك المحمول

قم بتعيين رمز مرور لجهازك المحمول حتى لا يتمكن الآخرون من الوصول إليه في حال فقدته. عند تثبيت تطبيق، اقرأ اتفاقية المستخدم. تكشف العديد من التطبيقات عن نوع المعلومات التي تجمعها وما قد تُستخدم من أجله. قد تقوم هذه التطبيقات بتعدين البيانات الشخصية، مثل بريدك الإلكتروني وموقعك وأنشطتك عبر الإنترنت. تأكد من المعلومات التي تتم مشاركتها قبل استخدام التطبيق حتى تشعر بالارتياح.

- التفكير ملياً قبل النشر

ما تنشره أو تقوله عبر الإنترنت يرسل رسالة عن هويتك، تمامًا كما يفعل ما يكشفه الآخرون عنك. قد لا ترسم سمات بصمتك الرقمية، مثل الصور التي تم تحميلها والتعليقات في المدونات ومقاطع فيديو YouTube ومنشورات Facebook، الصورة التي ترغب في أن تُرى بها. احرص على إنشاء بصمة رقمية إيجابية عن طريق نشر تلك الأشياء التي تسهم فحسب في تكوين الصورة التي تريد أن يراك الآخرون بها.

- التصرف بسرعة بعد انتهاك البيانات

إذا كنت تشك في أن بياناتك قد تم كشفها في حال حدوث انتهاك للبيانات، فاتخذ إجراءً على الفور. إذا كان الأمر ينطوي على خسارة مالية، فاتصل بالبنك أو بمقدم خدمات بطاقة الائتمان للإبلاغ عن الانتهاك. قم بتغيير أي كلمات مرور ربما تم كشفها. إذا كانت كلمة مرور استخدمتها لحسابات أخرى، فقم بتحديثها في جميع الحسابات.

- استخدام شبكة VPN

يمكن أن يساعد استخدام شبكة افتراضية خاصة أو شبكة VPN على سبيل الاختصار على حماية بصمتك الرقمية. وهذا لأن شبكات VPN تخفي عنوان IP الخاص بك، ما يجعل تصرفاتك عبر الإنترنت غير قابلة للتتبع فعليًا. وهذا يحمي خصوصيتك عبر الإنترنت ويمكن أن يمنع مواقع الويب من تثبيت ملفات تعريف الارتباط التي تتبّع سجل تصفح الإنترنت الخاص بك. يتيح لك Kaspersky Secure Connection الحصول على اتصال آمن بين جهازك وخادم الإنترنت بحيث لا يمكن لأحد مراقبة البيانات التي تتبادلها أو الوصول إليها.

الخاتمة :

إلى جانب الآثار السلبية للإستخدام المفرط للإنترنت ليس فقط عند الأطفال بل حتي عند الكبار ،فإن هذا الاستخدام في أغلب الأحيان يتسم بالآوعي و غياب أساسيات الأمن السيبراني ، فلا بد من تفعيل عدة إجراءات منها ما تتعلق بعقلنة الأفراد أثناء الاستخدام لهذه الوسائل التكنولوجية ،او ادراج برامج تدريبية للأمن السيبراني للكبار ة الصغار على حد سواء ،و تفعيل المجتمع المدني لمناقشة قضايا المشكلات الأسرية بعد تفاعلها مع هذه الوسائل التكنولوجية و التحديات التي واجهتها و تواجهها حاليا ،لإيجاد الحلول المناسبة من أجل تقليل الأضرار و الانعكاسات السلبية

1. ¹ نشوى عبد الغني (4100 .) إدمان الانترنت وعالقه ببعض الأعراض النفسية المرضية لدى طالب المدارس الثانوية . رسالة ماجستير غير منشورة . جامعة حلوان . كلية آداب . قسم علم النفس
2. ² - هند علي ليلة (4108 .) الفروق بين نمطي الإستخدام المفرط للإنترنت في إدارة الوقت والبحث الحسي . رسالة ماجستير غير منشورة . جامعة المنيا . كلية التربية . قسم الصحة النفسية
3. ³ نعمة محمد سيد عناني (4108 .) (الاستخدام السلبي لشبكة الانترنت وأثره في التفكك السري دراسة ميدانية إرتياد الزواج والزوجات لغرف الدردشة في محافظة الجيزة . رسالة ماجستير غير منشورة. جامعة القاهرة . كلية آداب . قسم إجتماع
4. ⁴ "Internet", Internet, Retrieved 19/4/2022. Edited. "Internet", Internet, Retrieved 19/4/2022. Edited. ↑ "What is the main source of Internet?", mvorganizing, 1/5/2021
5. ⁵ وسام عزت محمد (4100 .) إدمان الانترنت وبعض المشكلات النفسية الأكثر شيوعا لدى الجنسين دراسة سيكومترية كLINيكية . رسالة ماجستير غير منشورة . جامعة عين شمس . كلية التربية . قسم الصحة النفسية
6. ⁶ <https://alrai.com/article/449309/> ملاحق/التكنولوجيا-والعلاقات-الأسرية-انعكاسات-سلبية
7. ⁷ javatpoint, Retrieved 2/10/2021. Edited. ↑ "What are the disadvantages of the Internet?", computerhope, 7/6/2021, Retrieved 2/10/2021. Edited
8. ⁸ <https://me.kaspersky.com/resource-center/definitions/what-is-cyber-security>
9. ⁹ <https://me.kaspersky.com/resource-center/definitions/what-is-cyber-security>

10. Social media, screen time, and young people's) mental health, [Social media, screen time, and young people's mental health - The Lancet, Volume 393, Issue 10172](#)p611February 16, 2019)
11. ¹⁰ <https://cert.gov.sa/ar/awareness/iotsecurity/>
12. ¹¹ <https://me.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>
13. <https://www.skynewsarabia.com/business/1676021>