



حقوق الملكية الفكرية

الدليل مملوك للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلف وحقوق التأليف والنشر والطباعة، كلها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر. وعليه فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي أجزاء من هذا الدليل، أو الاقتباس منه، أو نسخ أي جزء منه، أو نقله كلياً أو جزئياً في أي شكل وبأي وسيلة، سواءً بطرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها سواءً من الأنظمة الحالية أو المبتكرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذن خطي منها.

ومن يخالف ذلك يُعرض نفسه للمساءلة القانونية.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدارة التميز السيبراني الوطني، الوكالة الوطنية للأمن السيبراني.

للاستفسار عن المبادرة أو البرنامج؛ يمكن التواصل عن طريق المواقع الإلكترونية أو الأرقام الهاتفية التالية:



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 <https://www.ncsa.gov.qa/>

✉ cyberexcellence@ncsa.gov.qa

☎ 00974 404 663 78

☎ 00974 404 663 62

الفهرس

07	الفصل الأول
	الأمن السيبراني والمخاطر الرقمية
09	• مقدمة
11	• أولاً: مفهوم الأمن السيبراني
23	• ثانياً: مفهوم المخاطر الإلكترونية
29	الفصل الثاني
	التحديات الرقمية
31	• مقدمة
33	• أولاً: خصائص الجريمة الإلكترونية
35	• ثانياً: البرمجيات الضارة
47	• ثالثاً: جرائم الشبكات
51	• رابعاً: القرصنة الرقمية
55	الفصل الثالث
	الخسائر الناتجة عن الهجمات الإلكترونية
57	• مقدمة
59	• أولاً: الخسائر على مستوى الدولة
65	• ثانياً: الخسائر على مستوى الشركات
69	• ثالثاً: الخسائر على مستوى الأفراد والأسر

75..... **الفصل الرابع**

التحديات الرقمية التي تواجه شرائح المجتمع

- 77..... • مقدمة
- 78..... • التحديات التي تواجه الأطفال
- 84..... • التحديات التي تواجه الشباب
- 90..... • التحديات التي تواجه الأسر

95..... **الفصل الخامس**

أسس مواجهة التحديات الإلكترونية

- 97..... • مقدمة
- 98..... • أهمية الاستراتيجيات الوقائية في الأمن السيبراني
- 100..... • أسس حماية الأطفال من المخاطر الرقمية
- 104..... • أسس حماية الشباب من المخاطر الرقمية
- 108..... • أسس حماية الأسر من المخاطر الرقمية

117..... **المراجع**

01

الفصل الأول

الأمن السيبراني والمخاطر الرقمية



■ مُقدمة

■ أولاً: مفهوم الأمن السيبراني

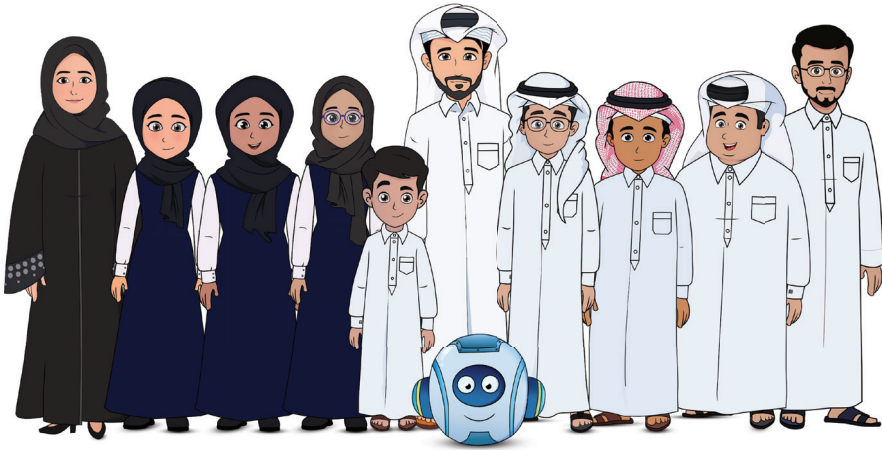
■ ثانياً: مفهوم المخاطر الإلكترونية

مقدمة

يُعَدُّ مفهـوم الأمان السيبراني والمخاطر الرقمية من المفاهيم الرئيسة في عالم الإنترنت، وتلقى هذه المفاهيم اهتمامًا متزايدًا، لا سيما في ظلّ تصاعد حدة التهديدات الرقمية التي تواجه مختلف شرائح المجتمع، والتقارير الدولية تشير إلى أنّ عدد الهجمات الرقمية التي تستهدف الأفراد تتزايد بشكلٍ حادّ، وهو ما ينسحب بشكلٍ مباشر على الأطفال واليافعين، وتؤكد هذه التقارير أنّ الأطفال واليافعين يُعدّون أهدافًا مفضّلة في عالم الجريمة الإلكترونية؛ وذلك كون هذه الشريحة لا تمتلك الوعي الكافي بقواعد الاستخدام الآمن للإنترنت، وهذا ما يُحتمّ العمل على تأهيل الأطفال بكيفية التعامل الآمن مع الإنترنت والأدوات التكنولوجية الحديثة.

التعامل الفعّال مع المخاطر الرقمية يعتمد بشكلٍ رئيس على الوقاية منها؛ فالأسلوب العلاجيّ بعد وقوع الهجمات يُعدّ مُنخفض الفاعلية، ويقتصر بشكلٍ رئيس على محاولة الإيقاع بالمُجرم ومُحاسبته، بينما بيانات الضحية تكون قد أُتلفت، والضرر قد تحقّق، لذلك لا بُدّ من التركيز على التأهيل والتدريب الرقمي لمختلف شرائح المجتمع، وفي مقدّمهم الأطفال واليافعون؛ كون التأهيل الرقمي يُعدّ أساس الحماية من المخاطر الرقمية، وهو جوهر الاستراتيجية الوقائية في الأمن السيبراني، فالتجارب الوطنية والدولية تشير بشكلٍ واضح إلى فاعلية الاستراتيجية الوقائية مقارنةً بنظيرتها العلاجية، وانطلاقًا من هذا الطرح، لا بُدّ من التركيز على نشر الوعي بمفاهيم الأمن السيبراني والسلامة الرقمية على مُستوى مختلف شرائح المجتمع، والتركيز على الأطفال واليافعين. يُعدّ التأهيل الرقمي للأطفال واليافعين مدخلًا رئيسًا للتأهيل الرقمي

على مستوى المجتمع ككل، فهم عماد المستقبل وركيزة التطور، وتأهيلهم رقمياً يعني رَفْد المجتمع مُستقبلاً بجيلٍ قادرٍ على التَّعامل الآمن والفعال مع الإنترنت والأدوات التكنولوجية الحديثة، ويُسهم ببناء مُجتمع آمن رقمياً وقادر على مُواجهة التَّحديات الإلكترونية والتَّعامل معها بفاعليَّة، واستناداً إلى هذا الطَّرح سيتمّ في هذا الفصل التَّعريف بأهمّ مفاهيم الأمن السيبرانيّ والسَّلامة الرِّقمية، والتَّعريف بالمصطلحات الرِّقمية الشَّائعة؛ بحيث يكون هذا التَّعريف مَدْخلاً للتَّعامل الفعال مع البيئة الرِّقمية، وأساساً للحماية من التَّحديات الإلكترونية.



أولاً: مفهوم الأمن السيبراني

يُعدّ مفهوم الأمن السيبراني من المفاهيم الحديثة، فعمره لا يتجاوز عُقودًا قليلة، ولكن وعلى الرغم من حداثة إلا أنه يلقى انتشارًا واسعًا على مستوى العالم أجمع، وعلى مستوى مختلف شرائح المجتمع، وذلك لكون تأثيره واسعًا ويّطال المجتمع ككلّ، لذلك لا بُدّ من التعريف الدقيق بدلالاته العلميّة والتّطبيقيّة، فمن النّاحية التّطبيقيّة من غير الممكن السّعي لتأهيل المجتمع رقميًّا بدون وجود وعي تامّ بمفهوم الأمن السيبراني والسّلامة الرّقميّة، فالخطوة الأولى في التّأهيل الرّقميّ للمجتمع عمومًا وللأطفال والياpecين على وجه الخصوص هي نشر معلومات دقيقة وحديثة حول الأمن السيبراني والسّلامة الرّقميّة والهجمات الإلكترونيّة وغيرها من المفاهيم ذات الصّلة.

مُصطلح الأمن السيبراني يتألّف من كلمتين: الأولى أَمْن، وهي نقيض الخوف، ويُقصد بها الاطمئنان والسّكينة، وشعور الفرد بالاطمئنان عند تعامله مع شيء ما، والكلمة الثّانية هي السيبراني، ويُقصد بها الفضاء الإلكترونيّ والإنترنت، وكلّ ما يتّصل بهما من مُستلزمات مادّيّة وغير مادّيّة، كالأجهزة والشّبكات والبرامج وغيرها، وكلمة سيبرانيّ مُشتقّة من كلمة Cybernetics التي تتّصل اصطلاحًا بعلم التّحكّم الآليّ والقدرة على التّحكّم بالآلة⁽¹⁾.

1. كمال، محمد، الإرهاب السيبرانيّ عندما يُستخدم الإرهابيّ الكيورد بدلًا من القبلة، دار كليم للطباعة والنّشر والتّوزيع (القاهرة - مصر)، ط1، 2022م، ص11.

المفهوم الاصطلاحي للأمن السيبراني

يُشير المفهوم الاصطلاحي للأمن السيبراني إلى القدرة على التعامل الفعال والآمن مع البيئة الرقمية، بهدف تحقيق الاستفادة القصوى من الفضاء السيبراني والقدرة على التعامل الفعال مع المخاطر والتهديدات الرقمية. والأمن السيبراني يرتبط بالقدرة على الحد من مخاطر الهجمات الإلكترونية التي من الممكن أن تتعرض لها الحكومات والشركات والأفراد، ويشير إلى التعامل الآمن مع الأجهزة الإلكترونية كالحواسيب والهواتف الذكية، والقدرة على حماية هذه الأجهزة والبيانات المخزنة بها من السرقة والتخريب والقرصنة، وحماية الشركات والأفراد من الجرائم الإلكترونية والابتزاز الرقمي، وتوفير مناخ آمن لتطور البيئة الرقمية في مؤسسات الدولة وفي المجتمع؛ ويشير الأمن السيبراني أيضًا إلى أي تقنية أو إجراء أو ممارسة لمنع الهجمات الإلكترونية والتخفيف من تأثيرها.

المفهوم التطبيقي للأمن السيبراني

من الناحية التطبيقية؛ يشير مفهوم الأمن السيبراني إلى مجموعة من السياسات والإجراءات التي يتم اتخاذها بهدف مواجهة التهديدات الإلكترونية التي تواجه الدول والشركات والمؤسسات والمجتمعات والأفراد، وبناء استراتيجيات تهدف لحماية البيانات والشبكات والبرامج من الهجمات الإلكترونية؛ بهدف سرقة بيانات يمكن أن تكون حساسة، مثل البيانات الشخصية والبيانات المالية والملكية الفكرية.

ويعمل الأمن السيبراني على مستويين؛ وقائي وعلاجي، يرتبط المستوى الوقائي بالعمل على تأهيل المؤسسات والأفراد على التعامل مع التهديدات الرقمية، واتباع إجراءات تحمي المؤسسات والأفراد من

الوقوع ضحية للجرائم الإلكترونية، فالمستوى الوقائي يهتم بالعمل على مواجهة الجرائم الإلكترونية قبل حدوثها، وقبل حدوث أي خسائر. أما المستوى العلاجي، فهو يهتم بالتدخل الفوري بعد حدوث الهجوم الإلكتروني؛ بهدف تقليل الخسائر إلى حدودها الدنيا، ومعالجة الأضرار التي سببتها هذه الهجمات، وبشكل عام، يعد المستوى الوقائي أهم من المستوى العلاجي وأكثر فاعلية منه؛ كون الأول يتدخل قبل حدوث أي هجوم وتسجيل أي أضرار، بينما في المستوى العلاجي تكون الخسارة قد تحققت والضرر قد وقع فعلاً.



المفهوم العلمي للأمن السيبراني

فيما يَخَصُّ التعريف العلمي بمفهوم الأمن السيبراني، فيُعرَّف بأنه: «مجموعة من العمليات والإجراءات التي وُضِعَتْ للدِّفاع ضدَّ هجمات قرصنة الحاسب الآلي، ويتَّصَلْنَ أيضًا وَضْعُ التدابير المطلوبة للحماية»⁽¹⁾.

كما يُعرَّف بأنه: «مجموعة من المهام والوسائل والسياسات والإجراءات الأمنية الموجهة لإدارة المخاطر، بالإضافة إلى تدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وبيانات المؤسسات والمستخدمين»⁽²⁾. ويُعرَّف أيضًا بأنه: «قُدْرَةُ النظام المعلوماتي على مقاومة محاولات الاختراق التي تُسْتَهْدَفُ البيانات»⁽³⁾.

وبشكلٍ عامٍّ يمكن تقسيم الأمن السيبراني لعدَّة قطاعات؛ بحيث تشمل مُجمِعةً مُختلف عناصر البيئة السيبرانية، وفيما يلي تبيان لأهم هذه القطاعات:

- **أمن الشبكات:** في هذا القطاع يهتم الأمن السيبراني بتأمين الشبكات من الهجمات الإلكترونية ومن التَّعدّيات الرقمية عليها، ويسعى للحفاظ على قاعليتها.

1. Lehto Martti, Neittaanmäk Pekka. Cyber Security: Analytics, Technology and Automation. Switzerland: Springer International Publishing, 2015.
2. Valeriano, Brandon and C. Maness, Ryan: "international relations theory and cyber security threats conflicts and ethics in an Emergent Domain in an emergent domain" in The Oxford Handbook of International Political Theory, edited by. Brown Chris and Eckersley Robyn. United Kingdom: Oxford University Press.
3. دحمانى، سليم، "أثر التَّهديدات السيبرانية على الأمن القومي... الولايات المتحدة الأمريكية أنموذجًا، 2017-2001م"، جامعة محمد بوضياف المسيلة، قسم العلوم السياسية، 2018م.

- **أَمْنُ التَّطبيقات:** يَهْدَفُ أَمْنُ التَّطبيقات لتوفير بيئة رقمية آمنة للتطبيقات؛ من خلال مُراعاة معايير الأَمْن الرقْمِيّ عند تصميم التطبيقات، بحيث لا يكون اختراقها سهلاً، كما يهتم هذا المحور بتصميم تطبيقات للحماية من الهجمات الرقْمِيّة والكشف عن البرمجيات الخبيثة وحذفها.
- **أَمْنُ المَعْلُومَات وسلامة وخصوصية البيانات،** في هذ المَحْوَ يهتم الأَمْن السَّيبرانيّ باتخاذ الإجراءات والتدابير اللازمة لَصَمان سلامة المعلومات والبيانات، وحمايتها من السرقة والقرصنة والتخريب.
- **الأَمْنُ التَّشغيليّ:** يرتبط هذا المحور بتوفير معايير الأمان الرقْمِيّ اللازمة للتعامل مع مُشغلي التّقنيات الرقْمِيّة، ومَنح إذن الوصول للبيانات المُهمّة والحسّاسة.
- **أَمْنُ المُستخدِم النّهائيّ:** وهو من المَحاور المُهمّة والرئيسة في الأَمْن السَّيبرانيّ، ويهتم بتوفير الأمان الرقْمِيّ للأفراد، وحمايتهم من المَخاطر التي قد يتعرّضون لها، مثل قرصنة البيانات الشّخصيّة وهجوم الفِدْيَة وغيرها من المَخاطر الرقْمِيّة⁽¹⁾.

1. What is Cyber Security? Kaspersky, on site: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>

وَيَرْتَبِط مَفْهُوم الْأَمْن السَّيْبِرَانِيّ بِعِدَّة مَفَاهِيم، وَمِنْ أَبْرَز هَذِهِ
المفاهيم ما يلي:

مَفْهُوم الْفَضَاء السَّيْبِرَانِيّ:

يُعرّف الفضاء السَّيْبِرَانِيّ على أنّه: "شبكة مُتَرايِطَة من البِنْيَة التَّحْتِيَّة المُولَّفة من تقنيات تخزين ومُعالِجة ونَقْل البيانات، إضافةً للشَّبكات والأجهزة التَّقْنِيَّة الدَّوْلِيَّة، والتي تُشْمَل الإنترنت وشبكات الاتِّصَالَات وأنظمة الحاسوب الآليّ ومختلف الأجهزة المتَّصلة بالإنترنت"⁽¹⁾، وبصِيفَة أُخرى، يُعدّ الفضاء السَّيْبِرَانِيّ هو البِنْيَة الرِّقْمِيَّة المُشكَّلة من مُختلف التَّقْنِيَّات والأجهزة والمُؤسَّسات والأفراد الفاعلين في العَالَم الرِّقْمِيّ، بمعنى أنّ أيّ قَرْد يَستخدَم الإنترنت يُعدّ جزءًا من الفضاء السَّيْبِرَانِيّ، ويؤثّر ويَتأثّر به.

الجريمة الإلكترونيّة:

هي مجموعة من الأفعال والأنشطة غير القانونيّة، والتي تهدف لتحقيق أهداف تتمثّل بإلحاق الضّرر بالحُكومات والشّركات والمُؤسَّسات والأفراد، وتتنعّد دَوَافِع الجريمة الإلكترونيّة، لتشمل تحقيق مكاسب ماديّة أو سياسيّة أو بهدف الابتزاز الماليّ أو الرِّقْمِيّ للضحايا، وفي ظلّ الانتشار المُتسارع للجريمة الإلكترونيّة على مستوى العَالَم، قامت العديد من الدُّوَل، ومنها دولة قطر، بسنّ قوانين وتشريعات تهدف لمُكافَحة الجريمة الإلكترونيّة ومُلاحقة مُرتكبيها، وبشكلٍ عامّ تُعدّ الوقاية من الجرائم الإلكترونيّة أكثر فاعليّة مقارنةً بالأدوات العلاجيّة، وذلك من

1. فرحات، علاء الدين. الفضاء السَّيْبِرَانِيّ: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونيّة والسياسيّة، المجلد العاشر، العدد الثالث، 2019م.

خلال توعية الأفراد بأسس الحماية الرقمية، وكيفية الحذر عند التعامل مع الإنترنت والأدوات التكنولوجية، فالوعي والتأهيل الرقمي يحمي الأفراد من الوقوع ضحية للجرائم الإلكترونية.

الهجوم السيبراني:

الهجوم السيبراني عمل غير قانوني، يستهدف تقويض استقرار الدول والشركات، وإلحاق الضرر بالأجهزة التقنية والشبكات والنظم التكنولوجية، وتعطيل الخدمات الرقمية العامة؛ من خلال استغلاله نقاط الضعف في الشبكات والنظم والتي تُعرف بالثغرات الرقمية⁽¹⁾؛ وذلك لتحقيق أهداف سياسية أو الابتزاز المالي، والعديد من الدول تتعرض بشكل مستمر لهجمات سيبرانية، قد تستهدف الحكومات أو الأفراد، ففي دولة قطر على سبيل المثال، تعرضت البلاد عام 2021م لأكثر من 15 مليون هجوم رقمي⁽²⁾.

-
1. أحمد عبيس نعمة، الفتلاوي. الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الأول، المجلد 44، 2020م، ص 49 - 76.
 2. الأمن السيبراني خلال كأس العالم: الجهود تتواصل لضمان فضاء سيبراني مفتوح وآمن في دولة قطر، مركز قطر للتطوير المهني، مُتاح على الرابط: <https://qcdc.org.qa/ar/fifa> الأمن-السيبراني-خلال-كأس-العالم-الجهو

أهداف الأمن السيبراني

يسعى الأمن السيبراني بشكل عام لتحقيق جملة من الأهداف، تتركز بشكل رئيس حول تعزيز الأمن الرقمي على مستوى الدولة والمؤسسات والأفراد، وفيما يلي تبيان للأهداف التفصيلية التي يسعى الأمن السيبراني لتحقيقها:

- ضمان الاستقرار الرقمي في مؤسسات الدولة، بما يشمل حماية أجهزتها وتطبيقاتها وبياناتها من الهجمات الإلكترونية، وضمان عمل أنظمة هذه المؤسسات على أكمل وجه؛ بحيث تكون قادرة على تقديم الخدمات المطلوبة منها.
- توفير الأمان والاستقرار للبيئة السيبرانية، وحمايتها من الهجمات الإلكترونية، بما يضمن مسار عمل رقمي مستقر في كل مستويات الدولة.
- حماية البنية التحتية الرقمية على مستوى الدولة والمؤسسات.
- معالجة الثغرات الرقمية والمعرفية الموجودة في البيئة السيبرانية، والتي من الممكن أن يتم استغلالها لتنفيذ هجمات إلكترونية.
- تعزيز ثقة الأفراد باستقرار البيئة السيبرانية.
- حماية الأفراد من الهجمات الإلكترونية بمختلف أشكالها.
- تعزيز الوعي لدى عموم أفراد المجتمع بمفاهيم الأمن السيبراني والسلامة الرقمية، وتقديم التدريب والتأهيل الرقمي لعموم المجتمع.
- توفير كافة المتطلبات التقنية اللازمة لمواجهة الجرائم الإلكترونية، والحد منها قدر المستطاع.
- الحد من تهديدات التجسس الرقمي ومخاطره الكبيرة، والتي تنعكس بشكل سلبي على حياة الأفراد وأداء المؤسسات.

-
- اتّخاذ كافّة التدابير لحماية المواطنين من مختلف المخاطر التي يُمكن أن يتعرّضوا لها خلال استخدام الأنظمة الرّقمية، وتصفّح شبكة الإنترنت بشكلٍ عامّ.



الأمن السيبراني وأمن المعلومات

عادةً ما يخلط بعض الأفراد بين مفهومي الأمن السيبراني وأمن المعلومات، وأنهما يحملان ذات الدلالة، ولكنهما في الحقيقة وعلى الرغم من اشتراكهما في بعض الجوانب؛ إلا أنهما يشيران لمفاهيم مختلفة، ويُعدّ أمن المعلومات أقدم من الأمن السيبراني، ويختصّ أمن المعلومات بحماية البيانات من التلف أو السرقة أو الضياع، والأخطار التي يهتم بها أمن المعلومات تُعدّ مُخفِضة مقارنةً بتلك التي يُعالجها الأمن السيبراني، ويعرف أمن المعلومات على أنه: مجموعة من الإجراءات والسياسات التقنية والإدارية، والتي تُستخدم لحماية البيانات الشخصية أو المؤسسية من أيّ تدخل مقصود أو غير مقصود أو غير مُصرّح به. ويهدف لحماية البيانات من الاستغلال والاستثمار غير المشروع⁽¹⁾.

كما يُعرّف أمن المعلومات على أنه الإجراءات والتدابير التي يتمّ اتباعها لحماية المعلومات، وحماية الأنظمة والأجهزة والتقنيات التي يتمّ استخدامها في تخزين ومعالجة البيانات، وترتبط المخاطر التي تواجه البيانات بمخاطر داخلية أو خارجية، فمجال اهتمام أمن المعلومات يقتصر على حماية البيانات والمعلومات من أيّ تهديد داخليّ أو خارجيّ، سواءً أكان هذا التهديد مقصودًا أم غير مقصود.

وبشكلٍ عامّ، يُعدّ أمن المعلومات جزءًا من الأمن السيبراني، بمعنى أنّ مجال عمل الأمن السيبراني أوسع وأشمل من أمن المعلومات، فالأمن السيبراني يهتمّ بحماية قطاعات أكبر وبيانات ومعلومات أكثر خطورة؛

1. سياسة إدارة البيانات، وزارة الاتصالات وتكنولوجيا المعلومات، دولة قطر، 2015م، مُتاح على الرابط: <https://www.mcit.gov.qa/ar/documents/document/da-ta-management-policy>

فهو يهتم بأمن كل ما يوجد في الفضاء الرقمي، وبالتالي يشمل أمن المعلومات، وحماية البيانات الإلكترونية وغير الإلكترونية جميعها.

يمكن اعتبار أمن المعلومات بمثابة أساس هدفه بناء أدوات وسياسات أمنية؛ لضمان سلامة البيانات السرية (مثل: البيانات الشخصية والمالية، وغيرها)، ويعتمد أمن المعلومات بشكل أساسي على ثلاثة معايير أساسية، وهي: السرية والنزاهة والتوافر. والهدف من السرية الحفاظ على خصوصية المعلومات الحساسة، والتأكد من أنها متاحة فقط للأشخاص المصرح لهم باستخدامها. أما النزاهة فتهدف لحماية البيانات من التعديل والتحريف، سواء عن طريق الصدفة أو عن طريق التعمد، أما التوافر فهو التحقق من أن البيانات الكاملة متاحة في كل مرة (أو في أي لحظة) عندما يحتاجها شخص مصرح له بالوصول إليها.



ويمكن توضيح الفُروق بين الأمن السيبراني وأمن المعلومات في النقاط التالية:

- يهتم أمن المعلومات بحماية البيانات المرفقة أصلاً على المنصات الإلكترونية. أما الأمن السيبراني فيهتم بحماية البيانات وحماية المستخدمين لها، وحماية وسائط التخزين التي يتم عليها تخزين البيانات، كما يهتم بوضع سياسات واستراتيجيات شاملة لحماية البيانات.
- يقوم أمن المعلومات بحفظ كافة البيانات الموجودة على التطبيقات التكنولوجية، أما الأمن السيبراني فيمنع التطبيق ذاته من التجسس على المستخدم أو تتبع عملياته على الإنترنت.
- أمن المعلومات لا يحمي البيانات من الخرق أو التجسس أو الإصابة بالفيروسات، لكن الأمن السيبراني يُشكّل نظام حماية إلكتروني لحماية الأجهزة نفسها وشبكات الإنترنت من استقبال أي نوع من أنواع الفيروسات والإبلاغ عنها.
- يقوم أمن المعلومات بتبليغ المستخدمين بأي محاولات لخرق البيانات، بينما الأمن السيبراني يمكنه تتبع المهاجم الإلكتروني، وتحديد هويته، وجمع المعلومات عنه؛ تمهيداً لمحاسنته قانونياً.
- يقوم أمن المعلومات بتوفير الحماية لصور وبيانات الأشخاص المصنّفين عامة على مواقع التواصل الاجتماعي، أما الأمن السيبراني فيمكنه الوصول إلى كافة البيانات والهويات التي وصلت إلى البيانات بطريق غير قانوني⁽¹⁾.

1. An Introduction to Information Security, Michael Nieves&Victoria Yan Pillitteri& Kelley Dempsey, June 2017, National Institute of Standard and Technology, U.S.Department of Commerce.

ثانيًا: مفهوم المخاطر الإلكترونية

يُقصد بالمخاطر الإلكترونية كل أنواع التهديدات التي من الممكن أن تتعرض لها المؤسسات أو الشركات أو الأفراد خلال تعاملهم مع البيئة السيبرانية، وترتبط المخاطر الإلكترونية بمجموعة من الهجمات والجرائم الرقمية التي تهدد المؤسسات والأفراد، كما ترتبط المخاطر الإلكترونية بمفهوم الهجوم السيبراني، والذي يُعرف على أنه عمل غير قانوني يقوم به شخص أو منظمة؛ لخرق نظام المعلومات الخاص بالآخرين، وعادة ما يكون الهجوم مدفوعًا بأغراض مادية، ولكن هناك أيضًا هجمات تتضمن سرقة البيانات أو المعلومات أو تعديلها أو تدميرها. بمعنى آخر، من بين أهداف الهجوم: تعطيل النظم الرقمية، أو سرقة بيانات الآخرين أو معلوماتهم، أو تعديلها أو تدميرها؛ ويرتبط الهجوم السيبراني بالجريمة الإلكترونية، والتي تُعرف بأنها: سلسلة واسعة من الأنشطة الضارة. ومن بين هذه الأنشطة: اعتراض البيانات بشكل غير قانوني، وانتهاكات حقوق الطبع والنشر، والتطوّل على النظام، مما يُضعف سلامة الشبكة وتوافرها⁽¹⁾.

ويمكن تعريف المخاطر الإلكترونية، وخاصة تلك التي يتعرّض لها الطلبة، بأنها: «المخاطر التي تهدد الأمن التربوي والأكاديمي للطلبة، وتنتج تلك المخاطر عن وجود خلل في التزام الطلبة بمعايير السلوك المناسب عند استخدام التكنولوجيا عبر الإنترنت، وذلك فيما يتعلق بحماية هويتهم

1. N. C. Hampson, "Hacktivism: A new breed of protest in a networked world" BC Int'l & Comp. L. Rev. vol. 35, p. 511, 2012.

ومعلوماتهم الشخصية، وقدرتهم على تمييز المواقع الخطرة التي يتعرضون لها، بما يؤثر سلباً على تحقيق الأهداف التعليمية بشكل سليم، ويؤدي بدوره إلى التأثير على قيم المجتمع وأخلاقه»⁽¹⁾.

وتشمل المخاطر الرقمية التي تواجه المجتمع بشكل عام، والطلبة بشكل خاص، طيفاً واسعاً من التهديدات، تشمل: التمر عبر الإنترنت، سرقة البيانات الشخصية، البرمجيات الخبيثة، التصيد الاحتيالي، وغيرها من المخاطر. وبشكل عام توجد عدة سياسات واستراتيجيات للحماية من المخاطر الرقمية، منها الاستراتيجيات الوقائية والعلاجية، وتعد الاستراتيجيات العلاجية منخفضة الفاعلية؛ لكون الهجوم الإلكتروني يكون قد حدث بالفعل، والخسارة قد تحققت، لذلك لا بد من الاعتماد على الاستراتيجيات الوقائية في التعامل مع المخاطر الإلكترونية، وتقوم الاستراتيجيات الوقائية على عدة مرتكزات، أهمها التدريب والتأهيل والتوعية، وذلك من خلال تقديم محتوى تدريبي وتوعوي للأفراد، بما يؤهلهم للتعامل الآمن والفعال مع الإنترنت والتقنيات التكنولوجية الحديثة، ويمكنهم من التعامل مع مختلف التهديدات الرقمية المحتمل مواجهتها خلال التعامل مع الإنترنت.

وللوقاية من المخاطر الإلكترونية، لا بد من الوعي التام بأنواعها وأشكالها، فهي لا تنحصر بشكل أو نوع واحد، بل تشمل عدة أنواع،

1. محمد حسين، سارة. إجراءات مقترحة لإدارة المخاطر السيبرانية، مجلة الإدارة التربوية، العدد الرابع والثلاثون، أبريل 2022م، ص 349.

وفيما يلي تبيان لأهم أنواع المخاطر الإلكترونية التي من الممكن مواجهتها خلال التعامل مع الإنترنت:

هجمات حجب الخدمة (DDoS):

وهي من المخاطر الإلكترونية التي تواجه الشركات والمؤسسات، لكنها تؤثر أيضًا وبشكل مباشر على الأفراد، وتهدف هذه الهجمات لتعطيل الخدمات التي تعتمد على شبكة الإنترنت؛ من خلال استهداف الشبكة وحجب الخدمة، وحاليًا يتم تقديم العديد من الخدمات العامة عن طريق شبكة الإنترنت، ولذلك فإن أي استهداف لهذه الشبكات يؤدي لحجب الخدمة، ما يلحق الضرر بالشركات والمؤسسات والأفراد.

هجمات التصيد:

وهي من التهديدات الإلكترونية التي تواجه الأفراد، وتهدف هذه الهجمات لسرقة البيانات الشخصية للمستخدمين، مثل كلمات المرور أو الصور والبيانات الشخصية الأخرى؛ لاستخدامها لاحقًا في ابتزاز الضحية وإلحاق الضرر به ماليًا واجتماعيًا ونفسيًا، وفي هذه التهديدات يعتمد المهاجمون على ضعف خبرة الضحية بقواعد الاستخدام الآمن للإنترنت، فعلى سبيل المثال: قد يتم إرسال برنامج خبيث للضحية عن طريق مرفقات البريد الإلكتروني، وفي حال تم فتح هذا المرفق يتم تثبيت البرنامج الخبيث في الجهاز، وتتم سرقة البيانات الشخصية للضحية.



هجمات برمجيات الفدية:

وهي نوع من أنواع التهديدات الإلكترونية الخطرة، والتي تعتمد على تثبيت برنامج خبيث في الجهاز الإلكتروني للضحية، وعندها يقوم البرنامج الخبيث بتشفير كل البيانات والمعلومات الموجودة على الجهاز، بحيث لا يتمكن المستخدم من الوصول إليها إلا في حال دفع فدية مالية للمهاجم.

هجمات تثبيت البرمجيات الضارة:

تعتمد هذه الهجمات على تثبيت برمجيات ضارة في جهاز الضحية؛ بحيث تقوم هذه البرمجيات إما بالتجسس على الضحية، أو بإتلاف بياناته، وتنتقل هذه البرمجيات عن طريق مُرَقَّقات البريد الإلكتروني أو عن طريق وسائط التخزين المصابة بهكذا برمجيات، أو عن طريق مواقع الإنترنت غير الموثوقة⁽¹⁾.

كل هذه التهديدات الرقمية لا يمكن أن تنجح في حال وعي المستخدم بقواعد التصفح الآمن للإنترنت، لذلك فمواجهة هذه التهديدات يعتمد بالدرجة الأولى على تعزيز الوعي بأنواع التهديدات وآلية عملها، وكيفية الوقاية منها، فالوقاية هي أفضل حل وأنجح أسلوب في الحماية من التهديدات الإلكترونية، لذلك لا بدّ من الحرص على التوعية والتأهيل بهذه المخاطر وبأسس التعامل الآمن مع الإنترنت.

-
1. Sanborn Colaco, How Can Educational Institutions Mitigate Cybersecurity Threats in Education? kitaboo, 18 Jul2023, on site: <https://kitaboo.com/how-educational-institutions-mitigate-cybersecurity-threats-in-education/>

02

الفصل الثاني

التحديات الرقمية



■ مُقدِّمة

■ أولاً: خصائص الجريمة الإلكترونية

■ ثانياً: البرمجيات الضارة

■ ثالثاً: جرائم الشبكات

■ رابعاً: القرصنة الرقمية

مقدمة

في ظلّ تطوّر أدوات التهديد الرّقميّ على مستوى العالم، باتت قضية تطوير أسس ومُرتكزات وأدوات الوقاية من الهجمات الإلكترونية ضرورةً مُلِحّة، خاصّةً في ظلّ تصاعّد الآثار الاقتصادية والاجتماعية والسياسية الناجمة عن الهجمات الإلكترونية، لذلك لا بدّ من الوّعي التّام بأنواع التهديدات الرّقمية وفهم كيفية تنفيذها؛ لكون الوّعي بهذه القضايا يعدّ مدخلًا للوّعي بكيفية الوقاية منها.

إنّ السّعي لتأهيل المُجتمَع رقميًا لا يمكن أن ينجح نجاحًا تامًا دون الفهم التّام لطبيعة التهديدات التي يُواجهها المُجتمَع عمومًا والأطفال على وجه الخصوص، فعلى سبيل المثال، من غير الممكن تحقيق الحماية من هجمات برامج الفدية دون المعرفة التّامة بهذه الهجمات وكيفية تنفيذها، وعلى العكس من ذلك، عند الفهم التّام لكيفية تنفيذ هذه الهجمات يُصبح من السّهل الوقاية منها، واستنادًا إلى هذا الطّرح، سيتمّ تخصيص هذا الفصل لدراسة أهمّ أنواع الهجمات الإلكترونية، وكيفية تنفيذها.



أولاً: خصائص الجريمة الإلكترونية

تختلف الجرائم الإلكترونية عن غيرها من الجرائم التقليدية بعدة نقاط، وتتميز عنها بعدة خصائص، ولا بُدّ لجميع شرائح المجتمع من الوعي بهذه الخصائص، وفيما يلي تبيان لأهمّ الخصائص التي تُميّز الجرائم الإلكترونية عن غيرها من الجرائم التقليدية:

تتمّ الجرائم الإلكترونية باستخدام أجهزة الحاسوب أو الهواتف المحمولة أو الأجهزة اللوحية؛

فالجريمة الإلكترونية تعتمد على الأجهزة التقنية في تنفيذ الهجمات الإلكترونية وتهديد الضحايا وابتزازهم.

جريمة خفية؛

فجزء كبير من الهجمات الإلكترونية تتمّ دون الإعلان عنها، وذلك إمّا لقدرة المجرم على إخفاء جريمته وعدم ترك أيّ دلائل على سرقته للبيانات، وإمّا لخوف الضحية من الإبلاغ، نتيجة اعتبارات عدّة، منها اجتماعية وثقافية، وهنا تظهر أهميّة دور البيئة المحيطة في تشجيع الأبناء على تقديم شكوى حول أيّ تهديد إلكتروني.

سرعة التنفيذ؛

فالجريمة الإلكترونية تتمّ في وقتٍ قصيرٍ للغاية قد يكون ثوانٍ معدودة، وهو ما قد يجعل هذه الجرائم غير محسوسة.

تتمّ عن بُعد؛

في ظلّ التطوّر التكنولوجي والعولمة الرقمية قد تتمّ بعض الهجمات الإلكترونية من دولٍ أخرى، فهي من الجرائم التي لا تعرف نطاقاً جغرافياً.

صعوبة المُحاسبة القانونيّة؛

المُلاحقة القانونيّة للجرائم الإلكترونيّة تُواجه صعوبات عدّة، لا سيّما إذا كان المُجرّم من بلدٍ مختلفٍ عن بلد الضّحية، وهذا ما يتطلّب تطبيق القوانين الدوليّة ذات الصّلة بالجرائم الإلكترونيّة.

صعوبة الإثبات؛

الجريمة الإلكترونيّة من الجرائم التي يصعب إثباتها؛ لأنّ المُجرّم لا يترك أيّ أثرٍ خلفه بخلاف الجريمة العاديّة، وحتى في حال وجود أيّ أثرٍ تقنيّ فإنّه فنيّا يصعب الاحتفاظ بهذا الأثر.

جريمة ناعمة؛

يُقصد بالناعمة أنّ الجرائم الإلكترونيّة تتمّ من خلال أدوات تقنيّة دون صخبٍ أو جُهدٍ عضليّ، على عكس الجرائم التقليديّة؛ فهي جريمة يمكن أن تحدث بكلّ سهولة باستخدام التقنيّات التكنولوجيّة الحديثة وفي أقلّ وقتٍ ممكن، وهو ما يُعزّز من خطورتها ويُصعّب من عمليّة مُلاحقتها.



ثانيًا: البرمجيات الضارة

وهي عبارة عن برمجيات خبيثة تتسلل إلى جهاز الحاسوب أو الهاتف الذكي في أثناء تحميل برامج أخرى، وتعمل على تدمير البيانات الخاصة بالأجهزة المستهدفة، وعادة ما يتم تثبيت هذه البرمجيات سرًا داخل النظام بغرض تعطيل البيانات؛ حيث تفقد البيانات سلامتها أو إمكانية الوصول إليها.

وتعد البرمجيات الضارة بمنزلة تهديد خارجي كبير للأنظمة؛ ويمكن أن تسبب أضرارًا وتعطيلات واسعة النطاق، كما يمكن أن تلحق خسائر كبيرة بالمؤسسات والأفراد، وعمومًا لا توجد أي شريحة اجتماعية في منأى عن هذه المخاطر، فأى استخدام للإنترنت ينتج عنه تعرض للمخاطر الرقمية، ومنها مخاطر البرمجيات الضارة، ولمواجهة هذه المخاطر لا بد من الوعي بها، وفهم دقيق لأنواع هذه البرمجيات وكيفية عملها وآلية استهدافها.

أنواع البرمجيات الضارة

البرمجيات الضارة هي مصطلح لجميع أنواع التهديدات الرقمية، فضمن البرمجيات الضارة تندرج أنواع كثيرة للتهديدات الرقمية، منها برمجيات التجسس وبرامج حضان طروادة وديدان الحاسوب وبرمجيات الفدية، وغيرها من البرمجيات الضارة، ولا بد لمستخدمي الإنترنت من الوعي التام بهذه الأنواع، وخصائص كل برنامج، وكيفية عمله وطبيعة الضرر الذي يسببه للضحية، وانطلاقًا من هذا الطرح تبين فيما يلي أهم وأبرز أنواع البرمجيات الضارة، ومبدأ عمل كل برنامج، وطبيعة الضرر الذي يسببه.

برنامج حصان طروادة Trojan horse

يُعدّ برنامج حصان طروادة من أشهر البرمجيات الضارة ومن أكثرها انتشاراً؛ إذ يتم الاعتماد عليه في تنفيذ عدد كبير من الجرائم الإلكترونية؛ وذلك لسهولة تثبيته على جهاز الضحية، فعند تحميل أي برنامج أو لعبة أو أغنية من موقع إنترنت غير موثوق قد يتم تحميل برنامج حصان طروادة دون معرفة المستخدم، ويبدأ البرنامج فور تثبيته بتغيير إعدادات الحاسوب أو الهاتف المحمول، ويبدأ سرقة بيانات المستخدم، وبشكل عام تُوجد أنواع كثيرة من برنامج حصان طروادة، وجميعها تشترك في آلية العمل، وفيما يلي تبيان لأهم هذه الأنواع:

حصان طروادة الخلفي:

في هذا النوع يقوم برنامج حصان طروادة بإحداث ثغرة رقمية في الجهاز، تُسمّى الباب الخلفي، ومن خلال هذه الثغرة يدخل المجرم إلى بيانات الضحية ويقوم بسرقتها.

هجوم حجب الخدمة الموزّع:

في هذا النوع يقوم البرنامج باستهداف الشبكات الرقمية، فيعطّلها أو يقوم من خلالها بالدخول إلى كلّ الأجهزة المتصلة بها، فمن خلال استهداف جهاز واحد يتم الانتقال عبر الشبكة إلى أجهزة أخرى.

برنامج حصان طروادة المزيّف لمكافحة الفيروسات:

يظهر هذا النوع كبرنامج حماية من البرمجيات الخبيثة (الفيروسات)، لكنّه في الحقيقة برنامج خبيث، وفور تثبيته يبدأ بسرقة بيانات الضحية وتعطيل جهازه.

بَرْمَجِيَّاتُ الْفِدْيَةِ

بَرْمَجِيَّاتُ الْفِدْيَةِ هِيَ نَوْعٌ مِنَ الْبَرْمَجِيَّاتِ الضَّارَّةِ الَّتِي تُهَدِّدُ الْمُسْتَعْمِلَ بِمَنْعِ الْوَصُولِ إِلَى بَيَانَاتِهِ، وَتُعْتَمِدُ هَذِهِ الْبَرْمَجِيَّاتُ عَلَى ضَعْفِ خُبْرَةِ الْمُسْتَعْمِلِ بِقَوَاعِدِ التَّصَفُّحِ الْأَمِنِ لِلْإِنْتَرْنِتِ، فَقَدْ تَثْقِلُ هَذِهِ الْبَرْمَجِيَّاتُ عَنْ طَرِيقِ قَنَحِ مُرَفِّقَاتِ الْبَرِيدِ الْإِلِكْتَرُونِيِّ الْوَارِدَةِ مِنْ مَصَادِرٍ مَجْهُولَةٍ، أَوْ مِنْ خِلَالِ تَحْمِيلِ بَرَامِجٍ أَوْ أَلْعَابٍ مِنْ مَوَاقِعٍ غَيْرِ مَوْثُوقَةٍ، وَقَوْرُ تَثْبِيتِ الْبَرَامِجِ الضَّارِّ يَقُومُ بِتَشْفِيرِ بَيَانَاتِ الصَّحِيَّةِ؛ بِحَيْثُ لَا يَتِمَكَّنُ مِنَ الْوَصُولِ إِلَيْهَا، وَلَا يَتِمُّ فَكُّ التَّشْفِيرِ عَنْهَا إِلَّا بَعْدَ دَفْعِ فِدْيَةٍ مَالِيَّةٍ يَطْلُبُهَا الْمُهَاجِمُ، وَبشكْلِ عَامٍّ يُوْجَدُ عِدَّةٌ مِنْ أَنْوَاعِ بَرْمَجِيَّاتِ الْفِدْيَةِ، وَلَا بُدَّ لِمُسْتَعْمِلِ الْإِنْتَرْنِتِ مِنَ الْوَعْيِ التَّامِّ بِهَا وَبِكَيْفِيَّةِ عَمَلِهَا؛ لِكُونَ الْوَعْيِ بِهَا يُؤَهِّلُهُ لِلْوَقَايَةِ مِنْهَا، وَفِيْمَا يَلِي تَبْيَانُ لِأَهْمِّ هَذِهِ الْأَنْوَاعِ:

بَرَامِجُ الْفِدْيَةِ الْمُشَفِّرُ WannaCry

هُوَ بَرَامِجُ فِدْيَةٍ مُتَسَلِّلٌ يَسْتَعْمِلُ ثَغْرَةَ أَمْنِيَّةٍ فِي بَرُوتوكُولِ Windows SMB، وَلَدَيْهِ آلِيَّةٌ نَشْرَ ذَاتِيٍّ تَسْمَحُ لَهُ بِإِصَابَةِ الْأَجْهَازَةِ الْآخَرَى؛ وَيُعَدُّ مِنْ أَبْسَطِ أَنْوَاعِ بَرْمَجِيَّاتِ الْفِدْيَةِ، وَاكْتِشَافُهُ وَإِزَالَتُهُ يُعَدُّ أَسْهَلَ مِنَ الْأَنْوَاعِ الْآخَرَى.

بَرَامِجُ الْفِدْيَةِ الْمُشَفِّرُ لِقْفَلِ الْبَيَانَاتِ Locky

بَرَامِجُ مُتَعَدِّدِ الْمِهَامِّ، وَقَادِرٌ عَلَى تَشْفِيرِ 160 نَوْعًا مِنَ الْمَلَفَّاتِ، وَتَمَّ إِصْدَارُهُ لِلْمَرَّةِ الْأُولَى عَامَ 2016م، وَغَالِبًا مَا تَتِمُّ الْإِصَابَةُ بِهِ عَنْ طَرِيقِ مُرَفِّقَاتِ الْبَرِيدِ الْإِلِكْتَرُونِيِّ؛ حَيْثُ يُرْسَلُ الْمُهَاجِمُ رِسَائِلَ بَرِيدٍ إِلِكْتَرُونِيِّ تُشَجِّعُ الْمُسْتَعْمِلَ عَلَى قَنَحِ مَلَفٍ MICROSOFT OFFICE WORD أَوْ EXCEL؛ إِذْ يَحْتَوِي هَذَا الْمَلَفُّ عَلَى بَرَامِجٍ خَبِيثَةٍ.

برنامج Cryptolocker

يُصيب عادةً أجهزة الحاسوب والهواتف الذكية من خلال البريد الإلكتروني ومواقع مشاركة الملفات والتّزيلات غير المحميّة، وهو لا يقوم بتشفير الملفات الموجودة على الجهاز المحليّ فحسب، بل يمكنه أيضًا فحص مُحركات أقراص الشّبكة المَعنِيّة وتشفير الملفات التي لديه إذن بالكتابة إليها، كما أنّ الإصدارات الجديدة من Cryptolocker قادرة على التّملّص من برامج مُكافحة الفيروسات وجدران الحماية⁽¹⁾.



1. What Is Ransomware? Proofpoint, on site: <https://www.proofpoint.com/us/threat-reference/ransomware>.

أُسُسُ الْوَقَايَةِ مِنْ بَرْمَجِيَّاتِ الْفِدْيَةِ

على الرَّغْمِ مِنْ خُطُورَةِ بَرْمَجِيَّاتِ الْفِدْيَةِ، فَإِنَّهُ مِنْ الْمُمْكِنِ بِسَهُولَةٍ الْوَقَايَةَ مِنْهَا، وَذَلِكَ مِنْ خِلَالِ اتِّبَاعِ جُمْلَةِ مِنَ الْقَوَاعِدِ الرَّقْمِيَّةِ الْخَاصَّةِ بِالتَّعَامُلِ مَعَ الْإِنْتَرْنِتِ وَالْبَيَانَاتِ، وَفِيهَا يَلِي تَبْيَانُ لِأَهَمِّ هَذِهِ الْقَوَاعِدِ:

النُّسخُ الْاِحْتِيَاظِيَّةُ لِلْبَيَانَاتِ:

إِنْشَاءُ نُسخٍ اِحْتِيَاظِيَّةٍ لِلْبَيَانَاتِ يُعَدُّ مِنْ أُسُسِ الْوَقَايَةِ مِنْ هَجَمَاتِ بَرْمَجِيَّاتِ الْفِدْيَةِ، فَفِي حَالِ تَعَرُّضِ الْبَيَانَاتِ لِلتَّشْفِيرِ يَكُونُ لَدَى الْمُسْتَحْدِمِ نُسخَةٌ أُخْرَى مِنْهَا؛ مَا يُقَلِّلُ الْأْضْرَارَ إِلَى الْحُدُودِ الدُّنْيَا.

الْحِفَازُ عَلَى تَحْدِيثِ نِظَامِ تَشْغِيلِ الْجِهَازِ وَبَرَامِجِ مُكَافَحَةِ الْبَرْمَجِيَّاتِ الضَّارَّةِ:

فِنْظُمُ التَّشْغِيلِ الْمَحْدَّثَةُ تَمْتَلِكُ عِدَدًا أَقَلَّ مِنَ الثَّغَرَاتِ الْأَمْنِيَّةِ، كَمَا أَنَّ التَّحْدِيثَ الْمُسْتَمِرَّ لِبَرَامِجِ مُكَافَحَةِ الْبَرْمَجِيَّاتِ الضَّارَّةِ (الْفَيروسَاتِ) يُعَدُّ مِنْ أُسُسِ الْحَمَايَةِ مِنْ هَجَمَاتِ بَرْمَجِيَّاتِ الْفِدْيَةِ.

اِسْتِخْدَامُ جِدَارِ الْحَمَايَةِ أَوْ جِدَارِ حَمَايَةِ تَطْبِيقَاتِ الْوَيْبِ (WAF)، وَأَنْظِمَةُ مَنَعِ التَّطَفُّلِ أَوْ كَشْفِ التَّطَفُّلِ (IPS/IDS):

فَهَذِهِ النُّظُمُ تُسَاعِدُ بِشَكْلِ مُبَاشِرٍ فِي الْحَمَايَةِ مِنْ هَجَمَاتِ بَرْمَجِيَّاتِ الْفِدْيَةِ⁽¹⁾.

1. What is Ransomware Attack? Imperva, on site: <https://www.imperva.com/learn/application-security/ransomware>.

برمجيات الإعلانات المتسللة

تُعَدّ الإعلانات جزءًا رئيسًا من الإنترنت، وغالبًا ما تقوم الشركات بجمع معلومات عن مستخدمي الإنترنت، وبناءً على اهتمام كلِّ مُستخدم يتمُّ توجيه نَقط مُحدّد له من الإعلانات، والمُجرمون الرّقميّون يَعْمَلُونَ على استغلال هذه الإعلانات لتفّيز هَجماتهم، فيتمُّ زرع برمجيات خبيثة ضمن الإعلانات، والتي يَنُتِج عنها أحيانًا اختطاف مُتصفّح الحاسوب بهدف التلاعب بمُحرّكات البحث والبدء بتتبُّع مهامّ الشبّكة، وتتمثّل تأثيرات برامج الإعلانات المتسللة فيما يلي:

- إبطاء الحاسوب: تُؤدّي الإعلانات المتسللة إلى بُطء الحاسوب؛ لكون الإعلانات تُستهلك جزءًا كبيرًا من قُدرة المُعالج ومن سرعة الإنترنت.
- إبطاء مُعالج الجهاز تُستهلك الإعلانات مساحة كبيرة من الذاكرة، وبهذه الطريقة تُؤدّي إلى انخفاض الأداء العامّ.
- الهجوم بالإعلانات: تُعَدّ الإعلانات مَصْدَرًا من مصادر التّهديد الإلكترونيّ، فمن خلالها يمكن للمُجرّم تثبيت برمجيات خبيثة على أجهزة الضّحية، ولكن لا يمكن أن يتمّ ذلك دون قيام المُستخدم بفتح نوافذ الإعلانات، فتجاهل الإعلانات يَحْمِي من هذه الهَجمات.
- توقّف البرامج عن العمل: إذا كانت البرامج تتوقّف عن العمل باستمرار، فهذا يعني أنّ نظامك مصاب ببرمجيات الإعلانات المتسللة.
- الاتّصال بالإنترنت بطيء: غالبًا ما تتراجع سرعة الاتّصال بالإنترنت في حال الإعلانات المتسللة؛ لأنّ عَرَض الإعلانات يَستهلك سرعة الإنترنت.

بَرْمَجِيَّات التَّجَسُّس

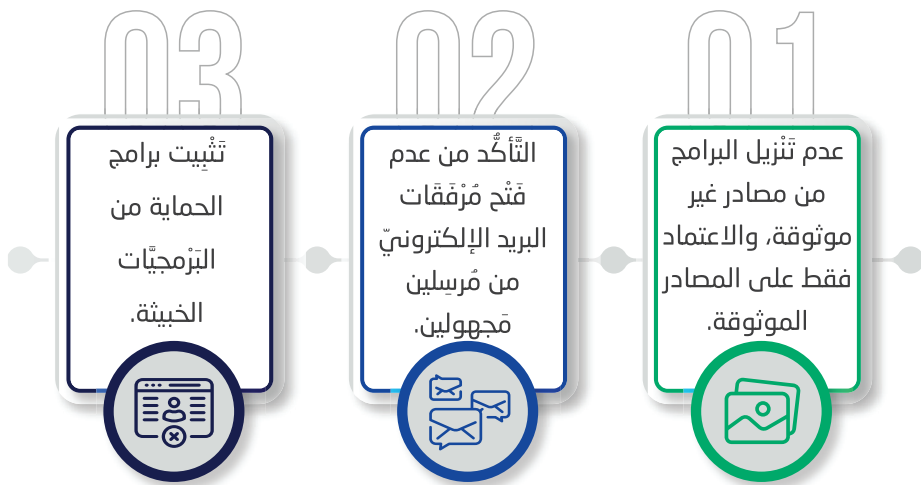
يُعَدُّ التَّجَسُّس الرَّقْمِيّ أَحَدَ الْمَخَاطِر الرَّئِيسَةِ الَّتِي يُوَاجِهُهَا مُسْتَخْدِمُو الإنترنت، وَيُعَدُّ مِنْ أخطر أنواع التَّهْدِيدَات الإلكترونية، لكون المُسْتَخْدِم لا يُلَاحِظ وجود بَرْمَجِيَّات التَّجَسُّس، فهذه البَرْمَجِيَّات تَبْقَى فِي الخفاء حتى بعد خرقها للجهاز⁽¹⁾، وتهدف بَرْمَجِيَّات التَّجَسُّس إلى سرقة بيانات المُسْتَخْدِم والاستفادة منها لاحقاً، كسرقة بياناته الشَّخصية لابتزازه لاحقاً والإضرار بِسُفْمَتِهِ، كما قد يتم استخدام البيانات المسروقة في جرائم التَّصَيِّد الاحتيالي والتَّسْمُر الإلكتروني.

ولبَرْمَجِيَّات التَّجَسُّس طُرُق عِدَّة لتحقيق أهدافها، فهي قد تَتَّبِع الكلمات التي يَكْتُبها المُسْتَخْدِم على لوحة المفاتيح، ومن خلال هذا التَّتَبُّع تقوم بسرقة كلمات المرور، أو قد تَدْخُل إلى مُحَرَّكَات الأقراص وتسرق الصُّور والبيانات الأخرى، وهي لا تُدَمِّر أيّ مَلَفَات، بل تَكْتَفِي بسرقتها؛ حتى لا يُلَاحِظ المُسْتَخْدِم وجودها.

وبشكلٍ عامٍّ، يختلف التَّجَسُّس الإلكتروني عن الهَجَمَات الرَّقْمِيَّة الأخرى في عِدَّة خصائص، أهمُّها الإفصاح، ففي هجوم الفِديَّة وبعد تَثْبِيت البرنامج الخبيث يتم إعلام المُسْتَخْدِم بأن بياناته قد تمَّ تَشْفِيرها، وأنَّه لن يتم فكَّ التَّشْفِير إلَّا بعد دَفْع الفِديَّة الماليَّة المطلوبة، بينما في بَرْمَجِيَّات التَّجَسُّس لا يقوم المُهاجم بإعلام الضَّحية، وقد يَنْتَهِي الهجوم دون معرفة المُسْتَخْدِم أنَّ بياناته قد سُرِقَت.

1. Kumar, G., Kameshwari, L. and Gunjan, V.K. (2021) Malware Techniques and Its Effect: A Survey, research gate, on site: https://www.researchgate.net/publication/360615209_Malware_Techniques_and_Its_Effect_A_Survey.

وللحماية من برمجيات التجسس، يمكن اتباع عدة قواعد، فيما يلي تبيان لأهمّها:



البرمجيات الخبيثة

يُطلق عليها "الفيروسات"، وهي برمجيات ضارة تعمل على تعطيل الأجهزة الإلكترونية، أو تدمير البيانات والملفات، وتتمثل خطورة هذه البرمجيات في أنَّ بإمكانها أن تنسخ نفسها بسهولة، ممَّا يؤدي إلى إصابة الأجهزة الأخرى بها في حال نُقل أيِّ ملفات من جهاز مصاب بها إلى جهاز آخر، فعلى سبيل المثال، في حال وجود ملفّ Word يَحْمِل برنامجًا خبيثًا؛ فإنَّ البرنامج الخبيث يَنْتَقِل إلى أيِّ جهاز آخر يتم فتح ملفّ Word عليه، وبشكل عامّ، تنتقل البرمجيات الخبيثة إلى الأجهزة من خلال عدّة طرق، فيما يلي تبيان لأهمّها:

في أثناء تحميل التطبيقات والبرامج:

تعدّ هذه الطريقة الأكثر انتشارًا، فغالبية البرمجيات الخبيثة تنتقل إلى الأجهزة عند تحميل تطبيقات من الإنترنت، وهذا الأمر يحدث فقط في حال التّحميل من المواقع غير الموثوقة، والأمر ذاته ينسحب على تحميل الألعاب والأغاني والفيديوهات والملفات.

مُرفقات البريد الإلكتروني:

وهي ثاني أكثر الطرق شيوعًا لانتشار البرمجيات الخبيثة، فيتم إرسال البرمجيات الخبيثة إلى الضحايا من خلال ملفات مُرفقة برسائل البريد الإلكتروني، وفي حال قام المُستخدم بفتح هذه المُرفقات فسيُنتقل البرنامج الخبيث إلى جهازه.

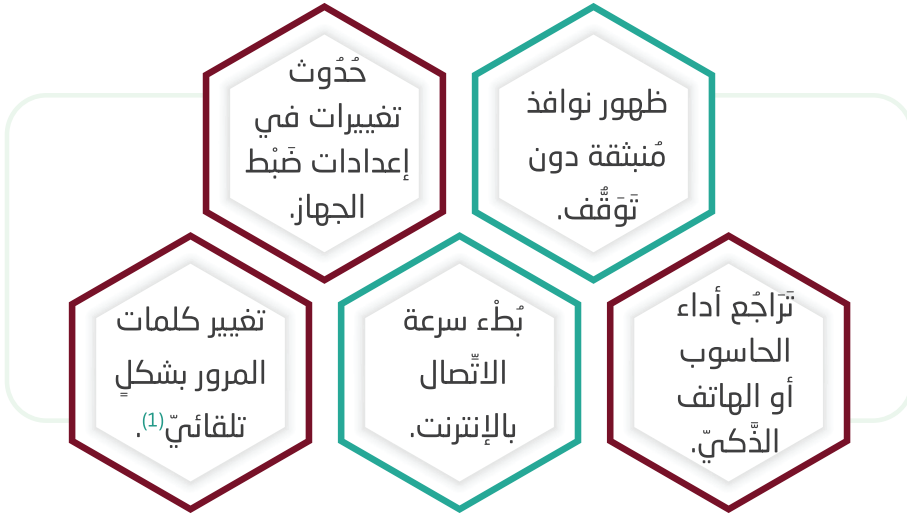
وسائط التخزين الخارجية:

مثل الأقراص الصلبة وحوايات الذاكرة الإلكترونية، ففي حال كانت هذه الوسائط مُتصلة بجهاز مصاب ببرنامج خبيث، فإنّها ستنتقل البرنامج إلى أيّ أجهزة أخرى تتصل بها.

الإعلانات الإلكترونية:

وهي الإعلانات التي تظهر على بعض مواقع الإنترنت، وهذه الإعلانات تُستخدم لتقل البرنامج الخبيث إلى الأجهزة المُستهدفة، وغالبًا ما يتم استخدام إعلانات تُثير قُصول المُستخدم لفتحها.

ويمكن التَّحَقُّق مِمَّا إذا كان جهاز الحاسوب أو الهاتف الذَّكي مُصابًا ببرنامج خبيث من خلال مُصادَقة المشكلات التَّالية:



1. What is Spyware? Kaspersky, on site: <https://www.kaspersky.com/resource-center/threats/spyware>.

بَرْمَجِيَّات ديدان الحاسوب

وهي برامج تُشبه البَرْمَجِيَّات الخبيثة، مع اختلاف رئيس هو أنها تستهدف الشبكات بشكل رئيس، ويمكن لهذه البَرْمَجِيَّات تَكَرَّار نفسها بسرعة كبيرة والانتشار في كامل الشبكات، ففي البداية تُصيب جزءًا مُحددًا من الشبكة، وسُرعان ما تنتقل بسرعة إلى بقية أجزاء الشبكات، وتهدف هذه البَرْمَجِيَّات إلى تعطيل الخدمات، مثل تعطيل الخدمات العامة التي تُقدَّم عن طريق الإنترنت، أو تستهدف سرقة البيانات السريّة التي يتم نقلها عن طريق الشبكة، مثل بيانات العملاء الماليّة، أو بيانات المرضى في المشافي، أو بيانات المؤسسات التعليميّة وغيرها⁽¹⁾.

برنامج Key logger

ويُسمّى أيضًا برنامج مُسجِّل ضربات لوحة المفاتيح، فمن خلال هذا البرنامج يتم مراقبة كل حرف، ورصد كل كلمة تُكتب من خلال لوحة المفاتيح، كما يعمل هذا البرنامج على التقاط لقطات من شاشة الجهاز وتسجيلها؛ والهدف منه هو التجسس على العمليات التي يقوم بها المُستخدم، كالتجسس على المُحادثات وانتهاك الخصوصية، أو سرقة البيانات الخاصّة بالعمليات الماليّة.

1. What is a Computer Virus or a Computer Worm? Kaspersky, <https://me-en.kaspersky.com/resource-center/threats/viruses-worms>.



ثالثاً: جرائم الشبكات

تُعَدّ جرائم الشبكات من التهديدات الرقمية الخطرة، ويُقصد بها تلك الجرائم التي يتم من خلالها مهاجمة الشبكات الإلكترونية بهدف سرقة البيانات منها، سواء أكانت تلك الشبكات خاصة بأفراد أم بمؤسسات، ويتم التعدي على الشبكات باستخدام البرامج الخبيثة التي تنتشر من تلقاء ذاتها، وتهدف جرائم الشبكات إلى تحقيق عدة أهداف غير قانونية، فيما يلي تبيان لأهمها:

- الاحتيال عبر البريد الإلكتروني والإنترنت.
- الاحتيال في الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها).
- سرقة البيانات المالية أو بيانات الدفع بالبطاقة.
- سرقة وبيع بيانات الشركات.
- الابتزاز الإلكتروني (المطالبة بالمال لمنع هجوم مهديد).
- هجمات برمجيات الفدية (نوع من الابتزاز الإلكتروني).
- التجسس الإلكتروني (حيث يصل المتسللون إلى بيانات الحكومة أو الشركة أو بيانات الأفراد).
- التدخل في الأنظمة بطريقة تعرض الشبكة للخطر.
- انتهاك حقوق الطبع والنشر.
- سرقة البيانات الشخصية للعملاء.
- تعطيل الخدمات العامة التي تقدم عن طريق الإنترنت.

أنواع جرائم الشبكات

لجرائم الشبكات أنواع عدّة، وكلّها تسعى لتحقيق هدفٍ رئيسٍ؛ هو إلحاق الضرر بالمؤسسات والأفراد، وتحقيق مكاسب مادية غير مشروعة، وفيما يلي تبيان لأهمّ هذه الأنواع:

هجمات حجب الخدمة (DDOS Attacks):

في هذا النوع من الجرائم يتمّ تعطيل الخدمات التي تتمّ عن طريق الشبكات، وينتج عن هذا الهجوم أضرار بالغة على المؤسسات والأفراد، ومنها على سبيل المثال، استهداف خدمات الأحوال المدنية التي تتمّ عبر الإنترنت.

هجمات الشبكات اللاسلكية (Wireless Attack):

في هذا النوع يتمّ استهداف الشبكات اللاسلكية بهدف تعطيل الخدمة، أو بهدف سرقة البيانات الشخصية للعملاء، ومنها على سبيل المثال، استهداف شركات شبكات الهاتف المحمول، بهدف سرقة بيانات العملاء وابتزازهم لاحقاً.

هجوم التوأّم الشرير (Evil Twin Attack):

يستهدف هذا الهجوم بشكلٍ رئيسٍ شبكات الـ WIFI المنزلية أو شبكات الشركات، وذلك من خلال خرق الشبكة، بهدف سرقة البيانات الحساسة، لا سيّما كلمات المرور الخاصة بالحسابات الشخصية، أو الصور والبيانات الشخصية من الأجهزة المتصلة بالشبكة، ويتمّ لاحقاً استخدام هذه البيانات لابتزاز الضحايا؛ ويسمّى هذا الهجوم التوأّم الشرير، لكون الهجوم يعتمد على إنشاء صفحة مُماثلة للصفحة الرئيسة للخادم؛ حيث لا يلاحظ المستخدم أيّ تغيير، فالصفحة المزيفة هي توأم للصفحة الأصلية.

هجمات سرقة البلوتوث (Bluejacking Attacks):

تستهدف هذه الهجمات الأجهزة التي تدعم تقنية البلوتوث، فيتم من خلال الشبكة زرع برمجيات ضارة في جهاز الضحية.





رابعًا: القرصنة الرقمية

يُقصد بالقرصنة الرقمية تنزيل وتوزيع محتوى محمي بحقوق الطبع والنشر دون الحصول على إذن قانوني، ويشمل ذلك التطبيقات والكُتب والمؤلفات الموسيقية وغيرها؛ بحيث يتم تحميل هذا المحتوى وتوزيعه دون إذن من الناشر أو المالك، بهدف تحقيق مكاسب مالية غير مشروعة، وهو ما يُعدّ من الجرائم التي يُعاقب عليها القانون في كثير من الدول، ومنها دولة قطر.

والقرصنة جريمة تطوي على خرق الأنظمة والوصول غير المصرح به إلى البيانات المخزنة، وترتبط عمليات القرصنة اليوم بشكل شائع بهجمات البرمجيات الضارة على الإنترنت والشبكات الأخرى، ويُطلق على الأشخاص الذين يُمارسون القرصنة الرقمية مصطلح «الهاكرز»؛ ولا تنتهي الآثار السلبية للقرصنة الرقمية عند مآلي الحقوق، بل تتعداهم لتشمل الأشخاص الذين يتعاملون مع البيانات والتطبيقات والمؤلفات المسروقة؛ فعند تحميل تطبيق من متجر غير رسمي، قد يكون هذا التحميل سببًا في الإصابة ببرنامج خبيث، وترتبط عملية التعامل مع البيانات المقرصنة كالكُتب والتطبيقات والأفلام والمؤلفات الموسيقية بجملة مخاطر، فيما يلي تبيان لأهمها:

الإصابة بالبرمجيات الضارة

أحد أبرز المخاطر الرئيسة للقرصنة الرقمية هو أنها تحمل برمجيات ضارة أو فيروسات يمكن أن تُسبب ضررًا للأجهزة.

الاحتيال عبر الإنترنت

ترتبط القرصنة الرقمية بشكل مباشر بالاحتيال عبر الإنترنت، فغالبًا ما تهدف القرصنة إلى الاحتيال على الضحايا، وسرقة بياناتهم الشخصية

بهدف ابتزازهم ماليًا، خاصّةً إذا تمّ تحميل برنامجٍ خبيثٍ عند تنزيل تطبيقاتٍ أو ملفّاتٍ من المواقع التي تعتمد على القرصنة الرقمية.

سرقة البيانات

سرقة البيانات الشخصية من المخاطر التي من الممكن مُواجهتها عند التعامل مع المؤلّفات والتّطبيقات التي تمّت قرصنتها رقميًا، ومن خلال سرقة هذه البيانات يتمّ ابتزاز الضّحايا ماليًا.



أُسُسُ الْوَقَايَةِ مِنَ الْقَرْصَةِ الرَّقْمِيَّةِ

تَنطَوِي الْقَرْصَةُ الرَّقْمِيَّةُ عَلَى جُمْلَةِ أخطار تَطَالَ حَقُوقُ الْمُؤَلِّفِينَ وَأَمَانُ الْمُسْتَعْدِمِينَ، لِذَلِكَ لَا بُدَّ مِنَ الْوَقَايَةِ مِنْ هَذِهِ الْأخطارِ، وَذَلِكَ بِاتِّبَاعِ النَّصَائِحِ التَّالِيَةِ:

تَحْمِيلُ الْمُؤَلَّفَاتِ الْمُخْتَلَفَةِ وَالتَّطبيقاتِ مِنْ مَوَاقِعَ رَسْمِيَّةٍ وَمُعْتَمَدَةٍ:

يَعْتَقِدُ بَعْضُ النَّاسِ أَنَّهُمْ يَتَّخِذُونَ قَرَارًا صَائِبًا بِتَحْمِيلِ الْمُؤَلَّفَاتِ وَالتَّطبيقاتِ مَجَّانًا مِنْ خِلَالِ الْمَوَاقِعِ الَّتِي تَعْتَمِدُ عَلَى الْقَرْصَةِ، لَكِنَّهُمْ بِذَلِكَ يَتَعَرَّضُونَ لِمَخاطر رَقْمِيَّةٍ تَتَمَثَّلُ فِي سُرْقَةِ بَياناتِهِمْ وَتَعَرُّضِهِمْ لِمَخاطر الْبَرْمَجِيَّاتِ الْخَبِيثَةِ، لِذَلِكَ لَا بُدَّ مِنْ تَحْمِيلِ الْمُؤَلَّفَاتِ وَالتَّطبيقاتِ مِنْ مَوَاقِعِهَا الرَّسْمِيَّةِ حَتَّى إِنْ كَانَتْ مَدْفُوعَةً، فَالْحَصُولُ عَلَى هَذِهِ الْمُؤَلَّفَاتِ وَالتَّطبيقاتِ مِنْ مَوَاقِعٍ تُقَدِّمُهَا مَجَّانًا يُعَدُّ مَخاطِرَةً كَبِيرَةً، إِضَافَةً إِلَى كَوْنِهِ انْتِهَاكًا لِحَقُوقِ الْمُؤَلِّفِينَ.

التَّثْقِيفُ وَالِدَّعْوَةُ ضِدَّ الْقَرْصَةِ الرَّقْمِيَّةِ:

تُعْزِيزُ الْوَعْيِ بِمَخاطرِ التَّعَامُلِ مَعَ الْمُؤَلَّفَاتِ الْمَسْرُوقَةِ يُعَدُّ مِنْ أُسُسِ الْحَمَايَةِ مِنَ الْمَخاطرِ الرَّقْمِيَّةِ، لِذَلِكَ لَا بُدَّ مِنْ نَشْرِ هَذِهِ الثَّقَافَةِ فِي الْمَجْتَمَعِ، وَالتَّرْكِيزُ عَلَى أَنَّ التَّعَامُلَ مَعَ الْمُؤَلَّفَاتِ الْمَسْرُوقَةِ يُعَدُّ مُخَالَفَةً قَانُونِيَّةً وَأَخْلَاقِيَّةً وَمَصْدَرًا مِنْ مَصَادِرِ التَّهْدِيدِ الرَّقْمِيِّ.

03

الفصل الثالث

الخسائر الناتجة عن الهجمات الإلكترونية



■ مُقَدِّمة

■ أَوَّلًا: الخسائر على مستوى الدَّولة

■ ثَانِيًا: الخسائر على مستوى الشَّرَكَات

■ ثَالِثًا: الخسائر على مستوى الأفراد

والأسر

مُقدِّمة

مع تَعَدُّ أشكال المَخاطر وتَنوُّع التَّهديدات الإلكترونيَّة تزداد حِدَّة الخسائر التي تُواجهها الدُّول والشَّركات والمُجتمعات والأفراد، وقد تَعَزَّز هذا التَّهديد مع الانتشار الواسع للإنترنت أفقياً وعمودياً، فغالبية المُجتمعات على مستوى العالم باتت تُستخدم الإنترنت بشكلٍ مكثَّف، وهو ما ينسحب على دولة قطر بشكلٍ مُباشر، فَنِسبة مُستخدمي الإنترنت في الدَّولة تتجاوز 99%⁽¹⁾، وبشكلٍ عامّ تتعدَّد أنواع التَّهديدات الإلكترونيَّة التي يُواجهها أفراد المُجتمع خلال تعاملهم مع الإنترنت، وتشمل الابتزاز المالي، وقرصنة البيانات الشخصية واستخدامها مِن قِبَل المُهاجمين لتحقيق مكاسب مائيَّة غير شرعيَّة، كما تشمل أيضاً: الابتزاز الاجتماعي، وقرصنة بيانات بطاقات الائتمان، وغيرها من الأشكال التي تُوصَف جميعها بأنَّها غير قانونيَّة وغير أخلاقيَّة.

وفي هذا الإطار، تجدر الإشارة إلى أنَّ مَخاطر التَّهديدات الإلكترونيَّة تتضاعف على مستوى الأطفال واليافعين، فهم الشَّريحة الاجتماعيَّة الأكثر عُرضة للمَخاطر الرِّقميَّة؛ بسبب صُغف خُبرتهم في التَّعامل مع التَّطبيقات التَّكنولوجيَّة، وهذا ما يجعلهم هدفاً سهلاً للقراصنة الرِّقميَّين.

1. قطر الأولى عالمياً في سرعة إنترنت الهاتف الجوال وفي استخدام شبكة الإنترنت، وكالة الأنباء القطريَّة، 9 مارس 2021م، مُتَّاح على الرِّابط: <https://www.qna.org.qa/ar-QA/News-Area/News/2021-03/09/0058-عالميا-في-سرعة-إنترنت-الهاتف-الجوال-وفي-استخدام-شبكة-الإنترنت>

وبشكلٍ عام، تُعدّ دراسة الخسائر الناتجة عن الهجمات الإلكترونية قضية بالغة الأهمية بالنسبة لتعزيز الوعي بأهمية مفهوم الأمن السيبراني والسلامة الرقمية، فالوعي التام بالخسائر الناجمة عن هذه الهجمات يُعدّ حافزاً للأفراد لاتباع قواعد التعامل الآمن مع الإنترنت، وذلك لتجنب الخسائر، وانطلاقاً من هذا الطرح؛ سيتم تخصيص هذا الفصل من هذا الدليل لدراسة وتوثيق أهم الخسائر الناجمة عن التهديدات الرقمية على أكثر من مستوى، بما يشمل الدول والشركات والمجتمع بمختلف شرائحه.



أَوَّلًا: الخسائر على مستوى الدولة

يشهد العالم تصاعّدًا واضحًا في الخسائر الاقتصادية الناجمة عن الهجمات الإلكترونية، ففي عام 2015م بلغت هذه الخسائر على مستوى العالم أجمع أكثر من 3 تريليونات دولار، وفي عام 2020م بلغت 8 مليارات دولار، وفي عام 2022م بلغت 10 مليارات دولار⁽¹⁾، ومن المُتوقَّع أن تبلغ 10,5 مليار دولار عام 2025م⁽²⁾.

وتشمل تكاليف الجرائم الإلكترونية: تَلَف البيانات وتَدميرها، وسرقة الأموال، وتَراجُع الإنتاجية، وسرقة المِلْكِيَّة الفِكرِيَّة، وسرقة البيانات الشَّخصِيَّة والماليَّة، والاختلاس، والاحتيال، وتعطيل المسار الطَّبيعي للأعمال، والتَّأثير على التَّحقيقات الجنائيَّة، واستعادة القرصنة وحَدْفهم للبيانات والأنظمة، والإضرار بالسُّمعة.

-
1. Kovacs, Eduard. Cybercrime Losses Exceeded \$10 Billion in 2022, security week, 13 March 2023, on site: <https://www.securityweek.com/cyber-crime-losses-exceeded-10-billion-in-2022-fbi/>
 2. Steve Morgan, Editor-in-Chief, Cybercrime to Cost The World \$10.5 Trillion Annually By 2025, cybersecurity ventures, 13 Nov 2020, on site: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

وعلى مستوى دُول العالم؛ تُعَدُّ الولايات المتحدة الأمريكية أكثر الدُول تَعَرُّضًا للهجمات الإلكترونية، كَوْنُهَا تعتمد على قطاع التكنولوجيا إلى حَدٍّ كبيرٍ، ففي عام 2021م تَعَرَّضَتْ أكثر من 30,000 شركة لهجمات إلكترونية، أمَّا على مستوى بيانات الأفراد، فقد تَجَاوَزَ عدد الهجمات التي تَعَرَّضَتْ لها البيانات الفردية 1,686 مليون هجوم في عام 2021م⁽¹⁾.

وفي إحصاءات عام 2022م كانت المملكة المتحدة أكثر الدُول من حيث عدد ضحايا الهجمات الإلكترونية، فقد زاد مُعَدَّل الهجمات على مُستخدمي الإنترنت بالدولة 40 بالمائة عن الإحصاءات الخاصة بعام 2020م، تلتها الولايات المتحدة الأمريكية، وتُعاني الولايات المتحدة من الجرائم الإلكترونية بشكلٍ كبيرٍ؛ حيث تمَّ خرق حسابات واحد من كلِّ اثنين من المستخدمين في 2021م، وبلغت خسائر ضحايا الابتزاز الإلكتروني في أمريكا عام 2021م أكثر من 13,6 مليون دولار⁽²⁾.

-
1. United States Cybersecurity Market - Growth, Trends, COVID-19 Impact, and Forecasts (2023 - 2028), mordor intelligence, on site: <https://www.mordorintelligence.com/industry-reports/united-states-cybersecurity-market>
 2. The Latest 2023 Cyber Crime Statistics (updated August 2023), available at: <https://aag-it.com/the-latest-cyber-crime-statistics/>

ومن أشهر نماذج الهجمات الرقمية التي تعرّضت لها الولايات المتحدة والتي أدّت إلى خسائر مائيّة كبيرة؛ الهجوم السيبرانيّ الذي أثر بشكل كبير على نتائج انتخابات 2016م في الولايات المتحدة الأمريكيّة، وأدّى إلى تحقيق خسائر مائيّة قدرها 35 مليون دولار أمريكيّ، ولم تتمكّن القيادة الأمريكيّة ولا المحقّقون في الأمر من اكتشاف الفاعل الحقيقيّ لهذا الهجوم الإلكترونيّ المؤثّر⁽¹⁾.

ووفقاً للمُنشدي الاقتصاديّ العالميّ فإنّ الخسائر على مستوى الدّول لا تتعلّق بالخسائر الماديّة فقط، وإنما تُؤدّي الهجمات الإلكترونيّة إلى وُجود تهديد عامّ غاية في الخطورة على دّول العالم، كما أنّها من العوامل التي تُسهم في زيادة مُعدّلات الهجرة غير الطّوعيّة التي يقوم بها الأفراد؛ هروباً من آثار الهجمات الإلكترونيّة، وما يترتّب عليها من آثار سلبية؛ نظراً لعدم الإبلاغ عن الجرائم أيضاً؛ إمّا لخوف الضحايا من التّعرّض للمخاطر أو لجهلهم بطريقة التّواصل مع السّلطات؛ حيث أكّدت وزارة العدل الأمريكيّة أنّه تمّ الإبلاغ فقط عن 25 بالمائة من إجماليّ الجرائم الإلكترونيّة التي تعرّض لها المواطنون في 2023م⁽²⁾.

-
1. الهجمات الإلكترونيّة (السيبرانيّة) والتّأمين، نشرة الاتحاد المصريّ للتّأمين، عدد رقم 67، لعام 2019م، مُتّاح على الرّابط: <https://cutt.us/gHPNu>.
 2. Steve Morgan, 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics, Cybercrime magazine, published at: <https://cybersecurityventures.com/cybersecurity-almanac-2023/>.

وتجدر الإشارة إلى أنَّ ألمانيا تعرّضت لحجم خسائر كبيرة في 2022م بسبب الهجمات الإلكترونية، حيث بلغت خسائر الهجمات الإلكترونية 206 مليارات يورو، وهو ما يعني تجاوز حجم الخسائر التي تتعرّض لها ألمانيا نتيجة الهجمات الإلكترونية حدّ 200 مليون يورو لثلاث سنوات متتالية⁽¹⁾.

ووفق إحصاءات عام 2022م كانت روسيا الاتحادية من أكثر الدّول التي تتعرّض للهجمات الإلكترونية على مستوى العالم أيضًا؛ حيث حظيت بـ 8.9% من إجماليّ الهجمات الإلكترونية في العالم عام 2022م، أمّا في عام 2023م فقد تراجعت تصنيفها لتحتلّ بـ 4.7% من إجماليّ الهجمات العالمية، وتركزت أبرز الهجمات الإلكترونية في روسيا على القطاع الماليّ للدّولة بنسبة 23% من إجماليّ الهجمات التي تتعرّض لها الدّولة، يليه قطاع الاتصالات بنسبة 19%، بينما حظي قطاع الترفيه بنسبة 15%، وقد زادت الهجمات التي تعرّضت لها قطاعات الدّولة المختلفة في روسيا بمعدّل 132% عن الإحصاءات السابقة؛ أمّا عن بقية الدّول الأكثر عُرضة للهجمات الإلكترونية في عام 2023م، فقد جاءت الولايات المتّحدة الأمريكيّة على رأس القائمة بنسبة 16.3% من إجماليّ الهجمات العالمية، وحظيت الهند بالمركز الثاني بنسبة 13.6%، وجاءت الصّين في المركز الثالث بنسبة 11.2% من إجماليّ الهجمات العالمية، أمّا فرنسا فكانت في المركز الرابع بنسبة 8.7%، وجاءت بريطانيا في المركز الخامس بنسبة 8.2% من إجماليّ الهجمات⁽²⁾.

-
1. The Latest 2023 Cyber Crime Statistics (updated October 2023), AAG, 2 October 2023, on site: <https://aag-it.com/the-latest-cyber-crime-statistics/>
 2. The Top 10 Countries Most Targeted by Cyberattacks, blogs, 2023, on site: <https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report>

وتواجه العديد من الدول بشكلٍ مستمرٍ آثارًا حادة للهجمات الإلكترونية، فعلى سبيل المثال: تعرّضت دولة كوستاريكا في عام 2022م لهجوم إلكترونيّ بفيروس فدية يُدعى "كونتي"، بعدة هجمات متتالية لعدة أشهر، وقد أدّى هذا الهجوم لشلّ حركة مختلف مؤسسات وقطاعات الدولة لدرجة أن مسؤولي الحكومة أعلنوا حالة الطوارئ في البلاد؛ نظرًا لهذا الهجوم شديد الخطورة، وقد أوضح بيان وزارة الخارجية في دولة كوستاريكا أنّ هناك 1000 جهة مُستهدفة تعرّضت لخسائر مباشرة نتيجةً لهذه الهجمات، وأن تكلفة هذا الهجوم وصلت 150 مليون دولار، ممّا يجعله من أغلى برمجيات الفدية على الإطلاق⁽¹⁾.

ويُتضح جليًا خطورة الهجمات الإلكترونية؛ لارتباط الأنظمة الحكومية وغير الحكومية بشبكة الإنترنت، وكيف أنّه تتمّ أغلب العمليات والخدمات المقدّمة للجمهور إلكترونيًا، وهو ما يعني أنّ تعرّض النظام أو الشبكة التي تقدّم الخدمات للجمهور لأيّ هجوم إلكترونيّ بمختلف أشكاله، سواءً أكان تجسّسًا أم هجوم فدية أم حتى تعرّضه لبرمجيات ضارة، من شأنه أن يؤدّي إلى حدوث خطرٍ كبيرٍ على بيانات المواطنين، وعلى النظام الأمنيّ العام للدولة.

-
1. How Conti ransomware hacked and encrypted the Costa Rican government, bleeping computer, on site: <https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/>

هذا الأمر يعني أنّ التّوعية بمخاطر الأمن السيبرانيّ لكلّ أفراد المجتمع أصبحت من الأمور الحثميّة لحماية الدّولة من المخاطر التي يُمكن أن تتعرّض لها في أيّ وقتٍ، خاصّةً مع تزايد تلك المخاطر بشكلٍ لحظيّ، ممّا يُوجب تطوير طُرُق مُواجهة الهجمات الإلكترونيّة التي تُعدّ من أكثر المخاطر التي تُعانيها دُول العالم في الوقت الحاليّ، سواءً على مستوى مخاطر الخسارة الماليّة التي تتزايد بشكلٍ حادٍّ من جراء الهجمات الإلكترونيّة، أو من خلال المخاوف الأمنيّة التي تُهدّد أمن الدّول واستقرارها.

ثانيًا: الخسائر على مستوى الشركات

تُعَدُّ الشركات من الأهداف المُفضَّلة للهجمات الإلكترونية؛ وذلك لأهدافٍ اقتصادية، أو في إطار المُناقَسة غير المشروعة بين الشركات، فعلى سبيل المثال: تعرَّضت مواقع إلكترونية لكبرى الشركات العالمية، لهجمات إلكترونية يوم 21 أكتوبر 2016م، ممَّا أدَّى إلى حدوث أعطال مُباشرة في هذه المواقع لمدَّة ساعتين، وهو ما أدَّى إلى تكبُّدها كثيرًا من الخسائر، وأشارت التقارير إلى مدى الأضرار الهائلة التي تعرَّضت لها الشركات نتيجة الهجمات الإلكترونية؛ حيث توقَّفت 60 بالمئة من الشركات الصغيرة والمتوسطة عن العمل نتيجة تعرُّضها لهذه الهجمات، وتراوحت مُعدَّلات الخسائر الماديَّة للشركات الصغيرة والمتوسطة بين 84 ألفًا و 148 ألف دولار أمريكي⁽¹⁾.

ووفق إحصاءات وتقديرات عام 2021م؛ يبلغ مقدار الخسائر التي تتكبُّدها الشركات نتيجة للهجمات الإلكترونية نحو 25 دولارًا في الدقيقة، وهو ما يعني حَجْم الخسائر الماليَّة الكبيرة للغاية، الأمر الذي دفع الشركات الكبرى إلى زيادة الإنفاق على الأمن السيبراني لديها بمُعدل وصل تقريبًا إلى 170 مليار دولار بزيادة سنويَّة مطَّردة⁽²⁾.

1. Lydon, Mark. 11 Companies Who Have Recently Faced a Cyberattack, Auto Grow, on site: <https://www.autogrow.co/recent-cyber-attacks-on-companies/>
2. Data Security Breach: 5 Consequences for Your Business, The Am Group, on site: <https://www.theamegroup.com/security-breach/>

جدير بالذكر أن خروقات البيانات مُستمرة في التطور بالنسبة للشركات؛ حيث تؤكد شركة Cybersecurity Ventures المتخصصة في مجال الأمن السيبراني أن كل 11 ثانية تقع شركة ضحية لهجوم إلكتروني، وهو معدل مرتفع عن مستوى الهجمات في 2019م؛ حيث كان يتم كل 14 ثانية، وتوقع الشركة أن يصل معدل الهجمات على الشركات إلى هجوم كل 2 ثانية في 2031م إذا استمرت الهجمات بهذا الوضع المتزايد؛ حيث دفعت بعض الشركات لمجرمي الإنترنت 40 مليون دولار لتنفيذ الهجمات الإلكترونية على الشركات في الدول الكبرى، ويعتقد أن مصدر هذا التمويل المالي للهجمات الإلكترونية على الشركات من روسيا⁽¹⁾.

وتُعاني الشركات في مختلف دول العالم من الهجمات الإلكترونية المُستمرة بهدف سرقة البيانات الخاصة بها، وتدميرها، أو طلب الفدية حتى يتم استرجاعها؛ حيث تعرضت 75% من الشركات الألمانية لهجمات إلكترونية في 2022م، فيما كانت النسبة في عام 2021م نحو 84% من الشركات لهجمات إلكترونية مما يعني وجود محاولات قوية من الدولة لتقليل معدلات الهجمات الإلكترونية على الشركات، ومحاولة الشركات ذاتها حماية أمنها السيبراني، ولكن هذه الهجمات من المؤكد تؤثر بشكل واضح على الأعمال الخاصة بالشركات وعلى وجودها داخل الأسواق⁽²⁾.

1. Steve Morgan, previous reference available at: <https://cybersecurityventures.com/cybersecurity-almanac-2023/>.
2. The Latest 2023 Cyber Crime Statistics (updated October 2023), AAG, 2 October 2023, on site: <https://aag-it.com/the-latest-cyber-crime-statistics/>

وَمِنَ الْمُؤَكَّد أَنَّ مَا تَتَعَرَّضُ لَهُ الشَّرَكَاتُ مِنْ خَسَائِرٍ مَالِيَّةٍ هِيَ خَسَائِرٌ كَبِيرَةٌ وَمُسْتَمِرَّةٌ؛ خَاصَّةً أَنَّ أَشْكَالَ الْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ الَّتِي تَتَعَرَّضُ لَهَا الشَّرَكَاتُ مُتَعَدِّدَةٌ وَمَخْتَلِفَةٌ، وَكُلُّ هَجْمَةٍ مِنْ هَذِهِ الْهَجَمَاتِ لَهَا أَثَرُهَا الْكَبِيرُ عَلَى الْوَضْعِ الْمَالِيِّ وَالْأَمْنِيِّ لِلشَّرْكَةِ. وَتَجْدُرُ الْإِشَارَةُ إِلَى ضَرُورَةِ تَوْعِيَةِ الطَّلَبَةِ بِأَنَّ كَافَّةَ أَنْوَاعِ الشَّرَكَاتِ تَتَعَرَّضُ لِلْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ؛ فَالْأَمْرُ لَا يَقْتَصِرُ عَلَى الشَّرَكَاتِ الْكَبِيرَةِ فَقَطْ، وَإِنَّمَا تَتَعَرَّضُ الشَّرَكَاتُ الصَّغِيرَةُ أَيْضًا لِهَجَمَاتٍ إِلِكْتَرُونِيَّةٍ مُتَتَالِيَةٍ؛ حَيْثُ تُوَاكِهَ الشَّرَكَاتُ الصَّغِيرَةُ 43% مِنْ نِسْبَةِ الْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ سَنَوِيًّا؛ حَيْثُ تُوَاكِهَ الشَّرَكَاتُ الصَّغِيرَةُ وَمُتَوَسِّطَةُ الْحَجْمِ خَسَائِرَ مَالِيَّةٍ كَبِيرَةً تُقَدَّرُ بِـ25 أَلْفٍ دُولَارٍ نَتِيجَةَ الْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ، وَوَفْقًا لِإِحْصَاءَاتِ عَامِ 2020م، وَصَلَ حَجْمُ الْخَسَائِرِ الْمَالِيَّةِ لِلشَّرَكَاتِ الصَّغِيرَةِ وَمُتَوَسِّطَةِ الْحَجْمِ حَوَالِي 2,8 مِلْيَارٍ دُولَارٍ فِيمَا نَحْوُ 700 أَلْفٍ هَجُومٍ تَعَرَّضَتْ لَهُ هَذِهِ الشَّرَكَاتُ.

وَوَفْقًا لِإِحْصَاءَاتِ عَامِ 2023م فَإِنَّ الشَّرَكَاتِ الصَّغِيرَةَ وَالْمُتَوَسِّطَةَ لَا تَزَالُ تُعَانِي مِنْ هَجَمَاتٍ قَوِيَّةٍ وَإِنَّ نِسْبَةَ قَلِيلَةٍ مِنْ هَذِهِ الشَّرَكَاتِ هِيَ الَّتِي تَمْلِكُ الْقُدْرَةَ عَلَى مُوَاجَهَةِ تِلْكَ الْهَجَمَاتِ، وَإِنَّ هَذِهِ الشَّرَكَاتِ تُنْفِقُ مَا بَيْنَ 653 - 826 دُولَارًا عَلَى حَوَادِثِ الْأَمْنِ السَّيْبِرَانِيِّ الَّتِي تَتَعَرَّضُ لَهَا، وَقَدْ قُدِّرَتْ نِسْبَةُ الْأَخْطَارِ الْبَشَرِيَّةِ فِي الْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ عَلَى الشَّرَكَاتِ فَوَصَلَتْ إِلَى أَنَّ 95% مِنْ الْهَجَمَاتِ بِسَبَبِ الْأَخْطَاءِ الْبَشَرِيَّةِ، وَمِنْ الْمُتَوَقَّعِ أَنَّ تَزْدَادَ التَّكْلِفَةُ الْمَذْكُورَةُ عَلَى الْهَجَمَاتِ الْإِلِكْتَرُونِيَّةِ 15% خِلَالِ السَّنَوَاتِ الْمَقْبِلَةِ لِتَصِلَ التَّكْلِفَةُ عَلَى الْإِنْفَاقِ عَلَى الْأَمْنِ السَّيْبِرَانِيِّ إِلَى 10,5 تَرِيلْيُونٍ دُولَارٍ بِحُلُولِ عَامِ 2025م⁽¹⁾.

1. Nivedita James, 51 Small Business Cyber Attack Statistics 2023 (And What You Can Do About Them), September 2023, on site: <https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/>



ثالثاً: الخسائر على مُستوى الأفراد والأسر

تتزايد مُعدّلات شكاوى الأفراد من الهجمات الإلكترونية في مختلف دُول العالم؛ حيث يُعاني كثير من الأفراد من التّعرّض لعمليات السرقة والابتزاز والتّهديد الرّقميّ، وعلى الرّغم من سَنّ دُول العالم عدداً من القوانين وتفعيل الإجراءات المختلفة للسيطرة على الهجمات الإلكترونية؛ إلّا أنّ الأمر فعلياً صَغَب للغاية وشديد الخطورة، ويَضُغَب التّحكُّم في تلك الهجمات؛ لأنّها في حالة ازدياد مُستمِرّ، فسرقَة البيانات الشّخصيّة للأفراد والأسر في الولايات المتّحدة الأمريكيّة أدّت إلى خسائر ماليّة تجاوزت 2,6 مليار دولار⁽¹⁾.

وتتعرّض الأسر في مُختلف دُول العالم للهجمات الإلكترونية لكون كلّ أفراد الأسرة تتعامل عبر الإنترنت؛ فمن المعاملات الماليّة لربّ الأسرة، والتي يُمكن أن يحدث فيها أيّ خطأ بشريّ بسهولةٍ يُؤدّي بدوْرِهِ إلى حدوث هجمات إلكترونيّة ضارّة، إلى تحميل الألعاب والبرامج من مختلف أفراد الأسرة والذي يُمكن من خلاله خرق الهواتف المحمولة، والتي تُؤدّي لمشكلات خطيرة مثل التّجسّس وسرقَة البيانات، وغيرها.

1. Internet Safety for Kids & Teens, Chapter 1: Cyber Threats to Kids & Teens, on site: <https://codesigningstore.com/cyber-threats-to-kids-and-teens>

وفيما يلي تبيان لأهمّ الخسائر التي تُواجه شرائح المجتمع نتيجة الهجمات الرقمية:

• الخسائر على مستوى الأطفال:

تؤكد الإحصائيات أن من بين كل 10 أطفال يتعرّض 6 أطفال للتّمر عبر الإنترنت، وفي عام 2020م سجّلت الجرائم الإلكترونية التي تستهدف الأطفال ارتفاعاً بمعدّل 144%، وبلغت الخسائر المالية السنوية الناجمة عن الجرائم الإلكترونية ضدّ الأطفال 660 ألف دولار أمريكي⁽¹⁾.

• الخسائر على مستوى الشباب:

يُواجه الشباب تحديات رقمية مُتصاعدة، والتي يَنُتج عنها خسائر حادة ومُتصاعدة، وجزء كبير من هذه الخسائر والتّحديات يتمّ تنفيذها من خلال منصات الألعاب الإلكترونية، ومن خلال جرائم التّصيد الاحتيالي، فوفقاً لموقع Kaspersky المُتخصّص بالأمان الرّقميّ، فإنّ عدد الشباب الذين تعرّضوا لهجمات رقمية عبر منصات الألعاب الإلكترونية بلغ عام 2022م أكثر من 7 ملايين هجوم، بزيادة سنوية بلغت 57%⁽²⁾، إضافة إلى ذلك فإنّ الاستعباد الإلكترونيّ يُعدّ من التّهديدات الخطيرة التي تُواجه الشباب على الإنترنت، ويُقصد بالاستعباد الإلكترونيّ أن يقوم المُهاجمون الإلكترونيّون بابتزاز الشباب مُقابل إجبارهم على العمل في مجال الجرائم

-
1. 6 out of 10 children exposed to cyber risks online, study finds, TRT world, 2021, on site: <https://www.trtworld.com/magazine/6-out-of-10-children-exposed-to-cyber-risks-online-study-finds-56733>
 2. Cyberattacks on young gamers up 57 percent in 2022, Kaspersky, on site: https://www.kaspersky.com/about/press-releases/2023_cyberattacks-on-young-gamers-up-57-percent-in-2022

الإلكترونية، ووفقاً لمنظمة الأمم المتحدة فإن ما لا يقل عن 200 ألف شخص أُجبروا على القيام بعمليات احتيال عبر الإنترنت⁽¹⁾، وذلك في إطار جرائم الاستعباد الإلكتروني.

• التحديات الرقمية التي تواجه الأسرة:

تواجه الأسر تهديدات إلكترونية مُتصاعدة، منها: ضعف العلاقات الأسرية نتيجة الإفراط في استخدام الإنترنت من قِبَل أفراد الأسرة، إضافةً لمخاطر سرقة البيانات الشخصية والبيانات المالية، وغيرها، وهذه المخاطر لها تبعات مالية، ففي الولايات المتحدة على سبيل المثال، أدت سرقة البيانات الشخصية لأفراد الأسر الأمريكية لخسائر تجاوزت 2,6 مليار دولار⁽²⁾؛ وهو ما ينعكس سلبيًا على المجتمع بالكامل.



-
1. جرائم الإنترنت تزحف لعالمنا الحقيقي.. والاستعباد الإلكتروني يأسر الآلاف، CNN، مُتاح على الرابط: <https://cnnbusinessarabic.com/technology/43132>؛ جرائم الإنترنت-تزحف لعالمنا الحقيقي-والاستعباد الإلكتروني-يأسر الآلاف
 2. Internet Safety for Kids & Teens, Chapter 1: Cyber Threats to Kids & Teens, on site: <https://codesigningstore.com/cyber-threats-to-kids-and-teens>



ولمواجهة التّحدّيات الرّقمية التي تُواجه عموم شرائح المجتمع، وللتّقليل من حدّة الخسائر التي تُسبّبها هذه المخاطر، لا بُدّ من اتّباع جُملة من إجراءات الوقاية الرّقمية، وأهمّها: اتّباع قواعد التّصفّح الآمن للإنترنت، تشمل هذه القواعد الإجراءات التّالية:

- كتابة كلمات مرور قويّة، وتغييرها بين الحين والآخر، وعدم استخدام كلمة مرور واحدة لكلّ الحسابات.
- تحميل البرامج والملفات من المواقع الرّسمية والموثوقة.
- عدم فتح المرفقات الواردة في البريد الإلكترونيّ من شخص مجهول.
- عدم الاستجابة للإعلانات التي تتحدّث عن ربح جوائز.
- عدم فتح الإعلانات المُنبثقة في المواقع الإلكترونيّة.
- استخدام جدار الحماية، وتثبيت برامج مُكافحة الفيروسات والبرمجيات الضّارة.

04

الفصل الرابع

التحديات الرقمية التي تواجه شرائح المجتمع



■ مقدمة

- التحديات التي تواجه الأطفال
- التحديات التي تواجه الشباب
- التحديات التي تواجه الأسر

مقدمة

على الرغم من التطور التكنولوجي المتسارع، وتطور مستوى الخدمات الرقمية التي بات يتمتع بها المجتمع؛ إلا أن الفضاء السيبراني يقترن بجملة تهديدات وتحديات تواجه المجتمع بمختلف شرائحه، فلاإنترنت جانب إيجابي وآخر سلبي، ومن الجانب التطبيقي لا يمكن تحقيق الاستفادة التامة من إيجابيات الإنترنت إذا لم نتكّن من التعامل الفعال مع التهديدات، لذلك لا بُدّ من تعزيز الوعي بأنواع المخاطر والتهديدات الرقمية التي تواجه الأفراد بمختلف شرائحهم عند استخدامهم للإنترنت، فالوعي والتأهيل والتدريب هو الأداة الفعالة التي من خلالها يمكن تحقيق الأمان الرقمي للمجتمع، وتعزيز القدرة على الاستخدام الآمن والفعال للإنترنت ولأدوات التكنولوجيا الحديثة، ولذلك وفي هذا الفصل من الدليل سيتمّ التعريف بأهمّ التهديدات الرقمية التي تواجه المجتمع، بدءًا من الأطفال مرورًا بالشباب فالأسر.

التَّهْدِيدات التي تُواجه الأطفال

يُعَدُّ الأطفال من أكثر الشرائح الاجتماعية تَعَرُّضًا للهجمات الرقمية؛ لكونهم الشريحة الاجتماعية الأكبر عددًا، إضافةً إلى كونهم هدفًا سهلًا للقراصنة الرقميين؛ نتيجةً لضعف خبرتهم في مجال السلامة الرقمية، فالإيقاع بهم يُعَدُّ سهلًا مقارنةً بالشرائح الأخرى، كما أن نسبتهم في الإنترنت تُعَدُّ الأكبر، فوفقًا لمنظمة الأمم المتحدة؛ فإن 33% من مستخدمي الإنترنت في العالم من الأطفال، كما أن أكثر من 175,000 طفل يستخدمون الإنترنت للمرة الأولى كل يوم⁽¹⁾، فهذه النسبة المرتفعة تُؤدِّي بالضرورة إلى ارتفاع مُعدَّل التَّهْدِيدات التي تُواجههم.

هذا، وتتَّعَدَّد أشكال وأنواع التَّهْدِيدات الرقمية التي تُواجه الأطفال، وفيما يلي تبيان لأهم هذه التَّهْدِيدات وأبرزها:

• التَّثَمُّر عبر الإنترنت:

يُعَدُّ التَّثَمُّر عبر الإنترنت من أبرز التَّهْدِيدات الرقمية التي تُواجه الأطفال، لا سيَّما خلال استخدامهم مواقع التَّواصل الاجتماعي، وتزداد أعداد الأطفال الذين يتعرَّضون لهذا الخطر، وتقدَّر نسبتهم بـ 33%⁽²⁾.

1. أكثر من 175,000 طفل يستخدمون الإنترنت للمرة الأولى كل يوم، مستفيدين من قرص كبيرة، ولكنهم يُعرَّضون أنفسهم لمخاطر جسيمة، الموقع الرسمي لمنظمة الأمم المتحدة، 6 فبراير 2018م، مُتاح على الرابط: <https://www.unicef.org/ar/البيانات-الصحفية/أكثر-من-175000-طفل-يستخدمون-الإنترنت-للمرة-الأولى-معرضين-مخاطر>

2. أبرز سبعة مخاطر يُواجهها الأطفال على الإنترنت: كيفية الحفاظ على أمنهم، kaspersky، مُتاح على الرابط: <https://me.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online>

• سرقة البيانات الشخصية للأطفال:

يواجه الأطفال على الإنترنت خطر سرقة بياناتهم الشخصية، وهذا التهديد قد يكون نتيجة لقلّة خبرة الأطفال بقواعد التعامل الآمن مع الإنترنت، أو نتيجةً لثغرات رقمية تقنية، فعلى سبيل المثال، تسببت شركة VTECH للألعاب التكنولوجية في سرقة بيانات أكثر من 6 ملايين طفل⁽¹⁾، وسرقة البيانات هذه قد تكون مدخلاً لتهديد جديد كالابتزاز الماديّ مثلاً. وقد تكون منصات الألعاب الإلكترونية التي تقبل التعامل بالعملة الرقمية المشفرة- مثل: Bitcoin- من مسببات سرقة البيانات الشخصية للأطفال؛ من خلال انجراف الطفل وراءها وإدلائه بمعلومات مالية وشخصية عنه أو عن أسرته، ممّا قد يؤدي إلى خرق الحسابات المالية للأسرة دون أن يدرك الطفل مدى خطورة الأمر.



1. Toy firm VTech hack exposes private data of parents and children, The Guardian, 30 November 2015, on site: <https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children>

• مَخَاطِر التَّعَرُّضِ لِمَحْتَوَى رَقْمِيٍّ خَطِيرٍ أَوْ غَيْرِ مُلَائِمٍ:

في العديد من المواقع الإلكترونية التي يتصفحها الأطفال عادةً، بما فيها مواقع التواصل الاجتماعي، قد يتعرّض الأطفال لمحتوى رقميٍّ سيئٍ أو غير مناسب، كالمحتوى المتطرف أو التحريض على العنف، أو المحتوى الذي يستعرض طرق إيذاء النفس، أو السلوكيات المُدمرة والعنيفة والأفكار العنصرية أو التمييزية؛ إضافةً للمحتوى المتضمن معلومات غير صحيحة أو غير دقيقة، وهذا ما تدعّمه وتؤكدّه التقارير والدراسات الدولية، ففي دراسة أجرتها منظمة اليونسيف عام 2020م، أكدت أنّ حوالي 80% من الأطفال يشعرون بخَطَر الاعتداء عبر الإنترنت⁽¹⁾.

• المَخَاطِر السلوكية:

تشمل المَخَاطِر السلوكية التحريض على النشاط العدائي وسط الأقران أو التسلُّط والتَّمرُّع عبر الإنترنت والمُطاردة الرقمية والابتزاز الإلكتروني⁽²⁾.

1. Growing Up in a Connected World, UNICEF, 2020, on site: <https://www.unicef-irc.org/growing-up-connected>

2. مُوجز السياسة العامة للحفاظ على سلامة الأطفال في البيئة الرقمية، الاتحاد الدولي للاتصالات، 2021م.

• مَخَاطِرِ الْبَصْمَةِ الرَّقْمِيَّةِ:

يُقْصَدُ بِالْبَصْمَةِ الرَّقْمِيَّةِ الظِّلُّ أو الأثر الذي يتركه كلُّ قَرْدٍ نتيجة استخدامه للإنترنت، بما في ذلك الأمور التي يبحث عنها والمواقع التي يزورها وما يكتبه على تطبيقات التَّوَاصُل الاجتماعيِّ، وهو ما يُعَبَّرُ عنه بالمقولة الثَّالِيَّة: "ما يُوضَع على الإنترنت يَبْقَى على الإنترنت"⁽¹⁾. وَالْبَصْمَةُ الرَّقْمِيَّةُ تُعَدُّ مَدْخَلًا لِلْمُهَاجِمِينَ وَالْمُجْرِمِينَ لاسْتِهْدَافِ الْأَطْفَالِ وسَرَقَةِ بَيَانَاتِهِم الشَّخْصِيَّةِ؛ وذلك كونهم الشَّرِيحَةُ الْأَقْلَى دِرَايَةً بِالْبَصْمَةِ الرَّقْمِيَّةِ وكَيْفِيَّةِ التَّعَامُلِ الْأَمِنِ مَعَهَا.

• مَخَاطِرِ الْإِدْمَانِ الرَّقْمِيِّ:

خَطَرُ الْإِدْمَانِ الرَّقْمِيِّ يُوَاجِهُهُ مُخْتَلِفُ شَرَاخِ الْمَجْتَمَعِ، لَكِنَّهُ أَكْثَرُ خَطَرًا عَلَى مَسْتَوَى الْأَطْفَالِ، وَيُشِيرُ مَفْهُومُ الْإِدْمَانِ الرَّقْمِيِّ إِلَى إِدْمَانِ اسْتِخْدَامِ الْإِنْتَرْنِتِ لِسَاعَاتٍ طَوِيلَةٍ، وَهُوَ مَا يُؤَدِّي لِنَتَائِجٍ سَلْبِيَّةٍ عَلَى عِدَّةِ مَسْتَوِيَّاتٍ؛ جَسَدِيَّةٍ وَنَفْسِيَّةٍ وَسُلُوكِيَّةٍ، كَمَا يُؤَدِّي إِلَى نَوْعٍ مِنَ الْاضْطِرَابَاتِ الَّتِي تُؤَثِّرُ عَلَى قُدْرَةِ الطِّفْلِ فِي التَّحَكُّمِ فِي انْدِفَاعَاتِهِ، وَتُشَبِّهُ أَعْرَاضَهُ أَعْرَاضَ إِدْمَانِ الْكُحُولِ وَالْمَقَامَرَةِ.

1. رحمين، نهاد، عتيقة كواشي. مقارنة التمكين المعلوماتي للمرأة: حماية الطفل من مخاطر المعلوماتية، مجلة الإحياء، المجلد 22، العدد 31، 2022م، ص 687.

ويُعدّ الإدمان الرّقميّ من المَخاطر التي قد تترك أثرًا نفسيًا وتربويًا سلبيًا لدى الأطفال، فتتحوّل الحياة بالنسبة لهم إلى أجهزة فقط، أجهزة الفيديو، الألعاب، والهواتف الذكيّة، ما ينتج عنه العديد من الأضرار، فالأطفال الذين يعانون من هذا الاضطراب غالبًا ما يَصلون إلى حالة من التّماهي والانسجام التّام مع الخيال الذي تُوفّره لهم تلك الأجهزة، وبالتالي يَخْلُق هذا ولعًا كبيرًا لديهم بكلّ التقنيات التكنولوجيّة، وما يمكن أن تُقدّمه لهم من واقع مُختلف، فيبدأ الطّفل في التمرّد على واقعه، والانعزال عن البيئة الاجتماعيّة التي تُحيط به، وهو ما يجعله غير راغب في مُمارَسة الأنشطة الجماعيّة، أو لا يمتلك نفس الاهتمامات التي يجب أن يمتلكها طُفل في هذه السّنّ.

ويميل الطّفل المُصاب بهذا الاضطراب إلى الجلوس لأوقاتٍ طويلةٍ وحيدًا؛ كي يتمكّن من استخدام هذه التقنيات كما يريد، وهو ما يُؤثّر على شخصيّته وحركاته وسلوكه؛ لأنّه بالطّبع يتأثّر بكلّ ما يراه، وبما أنّه يتابع ويُشاهد ما يُعرّض أمامه وحده ودون إشراف على الأغلب؛ سيتعرّض لكلّ أنواع المحتوى الضارّ والعنيف، والذي سيؤثّر عليه سلبيًا بكلّ الطّرق الممكنة.

والأمر ذاته يَنسحب على إدمان مواقع التواصل الاجتماعي، ما يُعزّز من شعور الطفل بالإحباط والقلق والتوتر؛ وفي حال وصل الإدمان الرقمي لمراحل مُتقدّمة فإنّ حرمان الطفل من الأجهزة الذكيّة ومن الوصول للإنترنت سيكون له أثر نفسيّ حادّ، ما يستدعي تدخّل الطبيب النفسي⁽¹⁾، لذلك لا بُدّ من توجيه الطفل ومُراقبته حتى لا يصل لمرحلة الإدمان الرقمي.



1. الشطري، حامد مجيد فارة. الإدمان الرقمي وعلاقته بالعزلة الاجتماعية لدى طفل طيف التوحد من وجهة نظر أولياء أمورهم، مجلة الباحث الإعلامي، العدد 56، كلية الإعلام، جامعة بغداد، العراق، ص 44، 45.

التَّهْدِيدَات التي تُواجهُ الشَّبَاب

يُعَدُّ الشَّبَاب هم الفئة الرّئيسة التي تُستخدم الإنترنت حول العالم، فبنسبة الذين يَتَمَكَّنون من الوصول إلى خدمات الإنترنت تبلغ 71%، ونسبة الشَّبَاب المُسْتخدِمين للإنترنت تبلغ 48% من إجمالي عدد السُّكَّان⁽¹⁾؛ ومع الاتِّساع الكبير في الفضاء السيبراني وتزايد الإقبال عليه انتشرت العديد من المَخاطر والتَّهديدات، والتي تنوّعت ما بين الجرائم الإلكترونيّة، والتَّنمُّر عبر الإنترنت، والاحتيال عبر الإنترنت، وغيرها من المَخاطر والتَّحديّات، وعلى الرّغم من أنّ كلّ هذه التَّهديدات طالت جميع مُستخدمي الإنترنت؛ إلّا أنّ الشَّبَاب هم الفئة الأكثر تضرُّراً بهذه الأمور؛ لأنهم الشَّريحة التي تُستخدم الإنترنت بشكلٍ يوميٍّ ولفتراتٍ طويلةٍ.

بخلاف هذا، انتشرت جرائم الإرهاب الرّقميّ واختراق المِلْكِيّة الفكرية والابتزاز، والعديد من أشكال القرصنة، والتي طالت الجميع؛ سواء الأفراد أو على مستوى المجتمع ككلّ، ومرةً ثانية يُعَدُّ الشَّبَاب المجنيّ عليه الأكبر في تلك الجرائم؛ لأنهم الأكثر تعلقاً والأكثر استخداماً للإنترنت؛ وهذا ما تُؤكِّده وتُعزِّزه الدّراسات والإحصائيّات الدّوليّة؛ فقد أكّدت دراسة أجرتها مُنظّمة اليونيسيف عام 2020م، أنّ ثلث الشَّبَاب الذين يَستخدمون الإنترنت تعرَّضوا للمَخاطر الرّقميّة⁽²⁾، وهو ما يُؤكِّد حَجْم المَخاطر والتَّهديدات التي يُواجهها الشَّبَاب على الإنترنت.

1. اليونيسيف: لتَجَمُّل العالم الرّقميّ أكثر أماناً للأطفال- مع زيادة الوصول إلى الإنترنت لتحقيق الفائدة للفئات الأكثر حرماناً، الموقع الرّسمي لمنظّمة اليونيسيف، 11 ديسمبر 2017م، مُتاح على الرّابط: <https://www.unicef.org/ar>
البيانات-الصحفية/الانترنت-لتحقيق-الفائدة-للفئات-الأكثر-حرماناً

2. Growing Up in a Connected World, UNICEF, 2020, on site: <https://www.unicef-irc.org/growing-up-connected>

وتتعدّد أشكال التّهديدات الرّقمية التي تستهدف الشّباب، وفيما يلي
تبيان لأهمّ هذه التّهديدات:

• التّمرّ عبر الإنترنت:

يواجه الشّباب مخاطر التّمرّ عبر الإنترنت بشكلٍ مُتزايد؛ فالإحصائيات
تقول: إنّ 21% من المُراهقين تعرّضوا للتّمرّ عبر الإنترنت⁽¹⁾؛ وغالبًا ما
يكون هدف التّمرّ عبر الإنترنت هو السيطرة على الضّحية أو إلحاق الضرر
النّفسيّ والمعنويّ به، وهو ما يُدخل الشّباب في أزمات نفسية حادة.

• الاتّجار بالبشر:

تعدّ مخاطر الاتّجار بالبشر من أخطر التّهديدات التي تواجه الشّباب، فوفقًا
لمنظمة الأمم المتّحدة؛ فإنّ المُتاجرين بالبشر يُعْتَرُونَ على ضحاياهم عن
طريق شبكات التّواصل الاجتماعيّ وألعاب الفيديو عبر الإنترنت⁽²⁾.

1. Ybarra, M. L. Linkages between Depressive Symptomatology and Internet Harassment among Young Regular Internet Users. *Cyber Psychology and Behavior*, (2), (2007). 247- 257.

2. المُتاجرون بالبشر يجدون ضحاياهم عبر مواقع التّواصل الاجتماعيّ وألعاب الفيديو، الموقع الرّسميّ لمنظمة الأمم المتّحدة، 21 أكتوبر 2021م، متاح على
الرّابط: <https://news.un.org/ar/story/2021/10/1085552>

• الانفتاح غير المدروس على الثقافة الغربية:

أدّى الإنترنت ومواقع التواصل الاجتماعيّ إلى انفتاح الشباب على الثقافات الأخرى، وهذا الانفتاح يُعدّ جيّدًا في حال كان مدروسًا ومُنظّمًا، ولكنّ في حال كان انفتاحًا تامًّا بدون ضوابط، فسيكون له تأثير سلبيّ على الشباب وعلى المجتمع بشكلٍ عامّ، خاصّةً أنّ الثقافات الأخرى قد تكون مُخالِفة للعادات والتقاليد السائدة في مجتمعاتنا.

• المُخدّرات الرقمية:

تُعدّ المُخدّرات الرقمية من أكثر التّهديدات الرقمية خطورةً على الشباب؛ خاصّةً أنّها تنتشر بسرعة، وتُعرَف أيضًا باسم Beats Binaural، وتُعدّ أحدث طريقة للإدمان النفسيّ، وتؤدي هذه المُخدّرات إلى إحداث تأثير على العقل والحواس؛ من خلال نغمات موسيقية قادرة على التأثير على دَبْذَبَات المُخّ الطبيعيّة، وتؤدي إلى الوصول إلى حالة من الاسترخاء السلبيّ، أو ربّما التّشّاط الرّائد، أو الوصول إلى حالة من الهدوء العميق وغيرها من التّأثيرات الغريبة وغير الطبيعيّة، وبالطّبع لا يوجد بعدّ قانون أو رقيب يمكنه المنع أو وضع حدّ لهذه الظّاهرة، على الرّغم من انتشارها وضرورة مُحاربتها، ولكنّ للأسف هناك حالة عامّة من تجاهلها والاستهانة بها وبتأثيراتها.

ومن خلال دراسة حالة الدماغ وطبيعة الإشارات الكهربائية التي تصدر عن الدماغ بعد تعاطي نوع مُحدّد من المُخدّرات يمكن تحديد طريقة النشوة المرغوبة، فكلّ نوع يستهدف نمطاً مُعيّناً من النشاط الدماغي، وبالطبع هناك العديد من العوامل التي تجذب الشباب للمُخدّرات الرقمية، خاصّةً أنهم يعتبرونها غير مؤذية مثل المُخدّرات العادية، فتلك المُخدّرات لا تعتمد على الموادّ الكيماويّة، كما أنّها لا تؤثر على الجسم، وغالباً ما تُعطي من يتعاطاها شعوراً بالاسترخاء والنشوة، ولا يشعُر من يتعاطاها بأيّ أعراض سلبية من تجربتها.

وتُعرض المُخدّرات الرقمية على العديد من المواقع الإلكترونيّة، والتي بالطبع يُقبل عليها الملايين؛ حيث يتخيّلون أنّها قادرة على الرّفْع من الحالة المزاجيّة وإعطاء من يتعاطاها نوعاً من السعادة، وتُستخدم أحياناً لإيقاف أو تنشيط الذاكرة الخاملة، وتُساعد في زيادة التخيّل والإلهام، كذلك تُساعد في رفع الأحاسيس بدون كحول⁽¹⁾.

1. سعيد محمود، آمال محمد، مخاطر المُخدّرات الرقمية على الشباب الجامعيّ ودور خدمة الجماعة في التخفيف منها، مجلة جامعة أسوان للعلوم الإنسانيّة، المجلد الثاني، العدد 2، مصر، 2022م، ص 96، 97.

هناك العديد من المَخاطر التي تقترب بالمُخدّرات الرّقمية؛ مثل الانطواء والانعزال عن الآخرين وعن العالم الواقعيّ، والدُّخول في حالة من الشُّرود الذّهنيّ، وزيادة التّعاطي تتأثّر كهرباء المخّ سلبيًا، ويقلّ التّركيز تدريجيًّا إلى حدّ فُقدان التّركيز تمامًا، وللأسف تنعكس تلك الأمور على الحالة الجسديّة فقد يُصاب المُدمن بالصّرع أو التشنّجات، وكذلك قد يُصاب بخلل في مراكز السّمع، وعلى مستوى السّلوّك يُصبح أكثر ميلاً للعدوانيّة، وتزيد تلك المُخدّرات الرّقمية من مُعدّلات الإصابة بالاكْتئاب، كما أنّها تُؤدّي إلى انخفاض كفاءة الذاكرة والانعزال عن الواقع تمامًا من أجل البحث عن النّشوة الرّائفة، وهنا يصل المُستخدم إلى الإدمان النّفسيّ، والذي لا يقلّ خطورةً أبدًا عن الإدمان على المُخدّرات التّقليديّة⁽¹⁾.

1. العراقي، صالح. تعرّض الشّباب الجامعيّ المصريّ للمواقع الإلكترونيّة التي تهتمّ بقضايا المُخدّرات وعلاقته بإدراكهم لمخاطر إدمان المُخدّرات الرّقمية، المجلّة العلميّة لبحوث الإذاعة والتلفزيون، العدد 11، مصر، ص 124.

• الإدمان الرقمي:

يواجه العديد من الشباب مخاطر الإدمان الرقمي، أي إدمان استخدام الإنترنت ومواقع التواصل الاجتماعي والألعاب الإلكترونية، ما يؤثر عليهم بشكل سلبي، ويحد من فاعليتهم في مجتمعاتهم، فنجد أن أغلب الشباب المفرطين في استخدام الإنترنت يصابون بمشكلات صحية تتمثل في اضطرابات النوم، واضطرابات التغذية، أمراض العيون، الشعور بالخمول والإصابة بالسممة والتهللات، وقد تصل مضاعفات تلك المشكلات إلى أمراض القلب والدماغ.

أما على مستوى الصحة النفسية فالإدمان الرقمي قد يؤدي إلى نوبات اكتئاب حاد، وعزلة، أيضا تتأثر العلاقات العائلية والعاطفية، فيكتفي كل منهم بالإنترنت أو ما لديه من تكنولوجيا ليستخدمها ويهمل في المقابل الدراسة والعمل، وتدرجيا تتغير السلوكيات والأخلاقيات بالطبع⁽¹⁾.

1. أحمد السيد، محمود علي، الإفراط في استخدام الإنترنت وبعض متغيرات الشخصية لدى طلاب الجامعة، مجلة دراسات عربية في التربية وعلم النفس، المجلد رقم 3، العدد 2، مصر، 2009م، ص 182، 183.

التَّهْدِيدات التي تُواجه الأسر

تُواجه الأسر تحدياتٍ كبيرةً مع تطوُّر العالم السَّيبرانيِّ والتَّقنيَّات الخاصَّة به، فليس كلُّ الآباء وأولياء الأمور لديهم الوَّعي الكافي بتمَّط الهجمات السَّيبرانيَّة ولا بطُرُق التَّعامل معها، وبالتالي فإنَّ عمليَّة توعية أولياء الأمور حول المخاطر والتَّهديدات السَّيبرانيَّة أمرٌ بالغ الأهميَّة، وهذه التَّوعية يمكنها أن تساعد على مُواجهة الآباء لهذه التَّهديدات، سواءً التي يمكن أن يفعلوا بها بأنفسهم أم التي يقع بها أبنائهم.

وفيما يلي تبيان لأهمِّ المخاطر الرِّقمية التي تُواجه الأسر:

• خطر التَّفكُّك الأسريّ:

إدمان الإنترنت يُعدّ مدخلاً للتَّفكُّك الأسريّ؛ لأنَّ كلَّ فردٍ منهم يعيش في عالمٍ افتراضيٍّ بعيدٍ عن الآخر، وهو ما يُؤدِّي إلى عدم تحقيق التماسك الأسريّ المطلوب، وفي هذا الشأن يمكن القول: إنَّ هناك علاقة عكسيَّة بين سوء استخدام الإنترنت، وبين مُعدَّل التَّوافق الأسريّ، بمعنى أنَّه كلما كان هناك انخفاض في مُعدَّل استخدام الإنترنت؛ فإنَّ ذلك يُؤدِّي إلى ارتفاع مُعدَّلات التَّوافق والانسجام بين أفراد الأسرة، والعكس صحيحٌ، ففي حال ارتفاع مُعدَّل استخدام الإنترنت؛ يقلُّ مُعدَّل التَّوافق والانسجام بين أفراد الأسرة الواحدة؛ والتَّهديد الرِّقميّ للأسر بلغ مرحلة بات معها يُهدَّد الأسرة ككيان اجتماعيٍّ، فإدمان الإنترنت كان سبباً في تفكُّك العديد من الأسر إضافةً لارتفاع عدَد حالات الطلاق.

• التأثير السلبي على منظومة القيم والأفكار:

أثر التحول الرقمي بشكل سلبي على القيم والأفكار والمواقف والاتجاهات، فبدلاً من الأسرة أصبحت مواقع الإنترنت والمؤثرون على منصات التواصل الاجتماعي وأصحاب المحتوى المصور هم المقدر الأول الذي يستمد المجتمع منهم أخلاقياته ومفاهيمه وقيمه وسلوكياته، وأغلبها مع الأسف تتعارض مع القيم والعادات المجتمعية السليمة؛ خاصة في ظل التعرض غير المنضبط لثقافات وقيم وأفكار تتعارض مع القيم والعادات السائدة في المجتمع، وهو ما يؤدي إلى فساد المجتمع بشكل عام.



• التأثير على الدور التربوي للأسرة:

الانشغال الكبير بالتكنولوجيا والتقنيات التي تعتمد على الإنترنت أدّى إلى إضعاف دور الأسرة في التنشئة، فكلّ يهرب إلى عالمه الرقميّ الخاصّ حتى الصغار، وهو ما أدّى إلى خلل في التوازن الاجتماعيّ، وأدّى إلى زيادة الانحراف الاجتماعيّ وزيادة التهديدات التي تتعرض لها مختلف أفراد الأسرة.

ويُعدّ فَقْدان التّواصل الأسريّ بسبب الإنترنت والعالم الرقميّ سبباً أساسياً في التأثير السلبيّ على الروابط العائليّة، فبدلاً من التّواصل مع أفراد الأسرة لدى الشخص عالم افتراضيّ كامل، يمكنه التّواصل معه، وبالطّبع قرّض هذا العالم الافتراضيّ الجديد قيمه الاجتماعيّة الجديدة والتي همّشت دور الأسرة بشكلٍ ملحوظ في عمليّة التّربية والقرّس الثقافيّ لتعيد تشكيل العقول والأفكار بما يتناسب مع هذا المجتمع الجديد. بالطّبع العزلة الاجتماعيّة كانت أحد الآثار السّليبيّة أيضاً للعالم الرقميّ، وكذلك زيادة شعور الأفراد باللامبالاة، فأصيبوا بحالة عزوف عن المشاركة في المجتمع؛ سواء المحليّ أو القوميّ.

إضافةً إلى ما سبق؛ فإنّ المخاطر الرقمية تتّسع لتشمل التحريض على العنف والتّخريب والتّطرف، فالإنترنت مليء بالمواقع التي تُحرّض على العنف، والتي لا تكتفي باستعراض الجرائم فحسب، بل يمكنها أن تُقدّم شرحاً مفصّلاً لطرق ارتكاب الجرائم، وطرق الهروب، وهو ما أدّى إلى زيادة الجرائم بشكلٍ كبير في العالم الواقعيّ.

ختامًا لهذا الفصل؛ لا بُدَّ من التأكيد على أنَّ الإنترنت والعالم الرِّقْمِيَّ له إيجابيّات تُفوق سلبيّاته، ويمكن الاستفادة منه في التعلُّم، والثّقافة، والفنون، وحتى في العمل، ولكنَّ الأمر كله يتوقّف على وَعْي المُستخدِمين وقُدّرتهم على التفريق بين الصّحيح والخطيئ، وقُدّرتهم على تجاوُز المساوئ والاستفادة بالإيجابيّات، وقُدّرتهم على الاستخدام المُتوازن للإنترنت والإمكانات الكثيرة التي وفّرتها التكنولوجيا، ولا يمكن أبدًا أن تُعفي الأسر من هذه المسؤوليّة؛ خاصّةً تجاه الأطفال والشّباب؛ لأنَّ هؤلاء هم رجال ونساء المُستقبل، وبالتالي على الأسرة أن تحافظ على وَعْيهم وعلى اعتدالهم وعلى المُوازنة في استخدام أدوات التكنولوجيا، لكي تعود للأسرة مَكانتها وقيمتها وقُدّرتها على الفِرس الثّقافيّ وتعليم الطّفل السلوكيّات والمعايير الصّحيحة والقيَم المجتمعيّة التي تضمّن صلاح المجتمع كُُلّ.

05

القَصْل الخامس

أُسُس مُوَاجَهَةِ التَّهْدِيدَاتِ الإِلِكْتروْنِيَّةِ



■ مُقَدِّمَةٌ

■ أَهْمِيَّةُ الْإِسْتِرَاطِيَّاتِ الْوَقَائِيَّةِ فِي

الْأَمْنِ السَّيْبِرَانِيِّ

■ أُسُسُ حِمَايَةِ الْأَطْفَالِ مِنَ الْمَخَاطِرِ

الرَّقْمِيَّةِ

■ أُسُسُ حِمَايَةِ الشَّبَابِ مِنَ الْمَخَاطِرِ

الرَّقْمِيَّةِ

■ أُسُسُ حِمَايَةِ الْأُسْرِ مِنَ الْمَخَاطِرِ

الرَّقْمِيَّةِ

مُقدِّمة

في ظلّ تصاعُد التهديدات الرقمية التي تُواجه مُختلف شرائح المجتمع، وفي ظلّ الخسائر الحادّة التي تُسببها الهجمات الإلكترونية؛ بات من الضروريّ مُواجهة هذه التهديدات، وتعزيز الأمان الرقميّ للمجتمع، ومُواجهة التهديدات الرقمية على مستوى مُختلف شرائح المجتمع، لا يمكن أن تُنجح دون تعاون أفراد المجتمع بالكامل؛ فالأمان الرقميّ مسؤوليّة فردية وجماعية في الوقت ذاته.

وبشكلٍ عامّ، ووفقًا للتجارب الدوليّة في مجال الأمن السيبرانيّ والسّلامة الرقمية؛ فإنّ الإستراتيجية الأكثر فاعليّة في مُواجهة التهديدات الرقمية، هي الإستراتيجية الوقائيّة، والتي تقوم على ضرورة التّدخل والتّصرّف قبل وقوع التهديد الإلكترونيّ، فالإستراتيجية العلاجيّة القائمة على التّدخل بعد وقوع الهجوم الرقميّ تُعدّ مُنخفضة الفاعليّة؛ كون الخسارة تكون قد وقعت، بينما في الإستراتيجية الوقائيّة يتمّ العمل قبل وقوع أيّ خسائر.

وبشكلٍ عامّ، لا يمكن أن تُنجح أيّ سياسة حكوميّة هادفة لتحقيق السّلامة الرقمية بدون تعاون أفراد المجتمع، لذلك على كلّ فرد العمل على تحقيق السّلامة الرقمية في المجتمع، كلّ من موقعه، والسّلامة الرقمية تتحقّق من خلال اتّباع جُملة من القواعد والسياسات النّاطمة للتعامل مع الإنترنت وتطبيقاته المختلفة، والتي تهدف في مجملها إلى مُواجهة التهديدات الإلكترونيّة المرتبطة باستخدام الإنترنت وتطبيقاته.

أهمية الاستراتيجيات الوقائية في الأمن السيبراني

في ظلّ زيادة حدة المخاطر الرقمية وكثرة الخسائر الناجمة عن الهجمات الإلكترونية؛ تزداد أهمية الإستراتيجية الوقائية في الأمن السيبراني، لا سيما في ظلّ تراجع فاعلية الإستراتيجية العلاجية، ففي الوقائية يتمّ التعامل مع التهديد الرقمي قبل وقوع الهجوم وحدوث الخسارة، لذلك فإنّ التعامل الفعال والأمن مع التهديدات الإلكترونية يجب أن يتمّ قبل التعرّض للهجوم الإلكتروني وليس بعده، وهذا صلب عمل الإستراتيجية الوقائية في الأمن السيبراني والسلامة الرقمية.

وهنا لا بدّ من التأكيد على أنّ "الصحة السيبرانية" يجب أن تكون مقياساً جديداً لاستعداد الدّول والمؤسسات والأفراد لمواجهة التهديدات الرقمية، وهو ما يتقاطع بشكلٍ مباشر مع جوهر وُصْلِب الإستراتيجية الوقائية في الأمن السيبراني. ويُقصد بالصحة السيبرانية أو الرقمية القدرة على الاستفادة التامة من الإنترنت والقدرة على مواجهة مخاطره بفاعلية⁽¹⁾.

وبشكلٍ عامّ تظهر أهمية الاستراتيجيات الوقائية في الأمن السيبراني والسلامة الرقمية من خلال النقاط التالية:

- اعتماد غالبية الدّول على خدمات الإنترنت، وهو ما يعني ضرورة حماية الشبكات من أيّ هجوم إلكترونيّ يؤدّي إلى خلل حادّ في العمل الحكوميّ قد يصل إلى مرحلة الشلل التام.

1. Andy Herman, MSIM, CISSP, Security and Infrastructure Intern West Monroe Partners, LinkedIn, 5 Jul 2016, on site: <https://www.linkedin.com/pulse/importance-cybersecurity-understanding-preventive-medicine-herman/>

- ضخامة الخسائر التي تتسبب فيها الهجمات السيبرانية، سواءً للدول أو للمؤسسات أو للشركات والأفراد، ما يجعل من الاستراتيجيات الوقائية أولوية أمنية واجتماعية واقتصادية وقومية.
- تنوع الهجمات السيبرانية وتعديدها وتطورها بشكلٍ لحظيٍّ، مما يُوجب ضرورةً مُواجهةً هذا التطور الخطير الذي يؤثر سلباً على كلِّ أفراد المجتمع ومؤسساته.
- حماية البيانات والمعلومات الخاصة بالدولة وبالأفراد، مما يعني حماية الأمن القومي للدولة والحفاظ على سلامتها وسلامة مؤسساتها وأفرادها.
- الحفاظ على الأنظمة والشبكات الإلكترونية من الاختراق.
- حماية الأفراد من خطر الابتزاز الإلكتروني والتهديدات المستمرة التي قد يتعرضون لها.
- العمل على اكتشاف نقاط الضعف المختلفة التي تُعانيها الأنظمة الإلكترونية والشبكات، والعمل على حلها ومواجهتها.
- التقليل من مُعدلات الأخطاء البشرية التي تساعد على زيادة الهجمات السيبرانية.
- توفير استراتيجيات الأمن السيبراني الوقائية بيئة عمل آمنة للموظفين في مختلف قطاعات الدولة.
- حماية الأفراد بمختلف شرائحهم من المخاطر الرقمية، وتعزيز مؤشرات الأمن السيبراني والسلامة الرقمية على مستوى المجتمع بالكامل.

أُسُس حماية الأطفال من المَخاطر الرقمية

نظرًا إلى المَخاطر التي يتعرّض لها الأطفال في البيئة الرقمية؛ أصبح من الضروريّ بناء أُسُس لحماية الأطفال من المَخاطر الرقمية، وتتمثّل أبرز هذه الأُسُس في بناء طفليّ واعيٍّ بالمواطنة الرقمية، وقادرٍ على التّعامل مع بيئة الإنترنت؛ وذلك من خلال تنمية المهارات الرقمية لدى الأطفال، والعمل على تطوير قُدّراتهم الخاصّة في التّعامل مع المواقع الإلكترونيّة بشكلٍ آمن.

وفيما يلي تبيان لأهمّ أُسُس حماية الطّفل من المَخاطر الرقمية:

• زيادة الوعي بمفاهيم الأمن السيبرانيّ والسّلامة الرقمية:

من أهمّ أُسُس حماية الأطفال من المَخاطر الرقمية هو العمل على تعليمهم وتوعيتهم بشأن هذه المَخاطر؛ من خلال إدراج طُرُق تدريس ومناهج تشمل البيئة الرقمية وطُرُق التّعامل معها، وكذلك العمل على تقديم تدريب عمليّ للأطفال يُمكنهم من التّعامل السّليم مع البيئة الرقمية، وتعريضهم لبعض المواقف المُفتّلة، وقياس مدى صحّة تعاملهم مع المواقف الإلكترونيّة التي يمكن أن يتعرّضوا لها، وتقديم توجيّه من المُعلّم والمُدرب إلى طريقة التّعامل الصّحيح مع المَخاطر الرقمية التي يمكن أن يتعرّض لها الطّفل.

• المُشاركة:

ويُقصد بها مُشاركة الطُّفل في إيجاد حُلُول لبعض المشكلات والمواقف الرِّقمية التي يمكن أن يتعرَّض لها هو أو يتعرَّض لها زملاؤه، أو مُشاركته في المواقف المُفتعلة التي يمكن تصميمها لتدريب الأطفال على كَيْفِيَّة التَّعامل معها؛ كما يتِم في هذا الإطار مُراقبة الأطفال أثناء استخدامهم للهواتف الذِّكيَّة، ومُراقبة المواقع الإلكترونيَّة التي يدخلونها.

• دَعْم المختصِّين في بناء برامج توعية للآباء والمُعَلِّمين:

ووضَّع سياسات يمكنها تطوير سُبُل الحماية الرِّقمية للأطفال، مِن قِبَل المختصِّين في البحث العلميِّ بهذا المجال.

• إعداد ضمانات لحماية التَّجربة الرِّقمية للطُّفل

والتي تشمل إنشاء كلمات مرور قويَّة ليس من السَّهل تخمينها، وكذلك تَشغيل إعدادات الخصوصية والأمان، مثل تشغيل إعدادات البَحْث الآمن؛ حيث تُقدِّم معظم مُحرِّكات البحث مثل Google إعدادات "البَحْث الآمن" الذي يُساعد على إخفاء النَّائج غير المُناسِبة، واستخدام أدوات الرِّقابة الأبويَّة، وكذلك وَضْع حُدود على وقت الشَّاشة، وتصفية المحتوى غير المُناسِب، ومنعهم من استخدام تطبيقات ومواقع ويب مُعيَّنة، ومن إجراء عمليَّات شراء داخل التَّطبيق.

أيضاً، يَدْخُلُ في هذا الإطار استخدام مَنَصَّاتِ صَدِيقَةِ اللِّطْفِ، مثل المواقع ومُحرِّكات البحث المُلَائِمَةِ للأطفال مثل YouTube و KidzSearch Kids وما إلى ذلك للمُساعدَةِ في تَصْفِيَةِ المحتوى الرِّقْمِيِّ.

- **تدريب وتوعية الأطفال بضرورة إطلاع ذويهم على كل ما يلاحظونه على الإنترنت:**

فالأطفال، ومن خلال تَعَامُلِهِمْ مع الإنترنت، وفي ظلِّ خِبْرَتِهِمْ المَحْدُودَةِ في التَّعَامُلِ مع المَخَاطِرِ الرِّقْمِيَّةِ؛ لا بُدَّ من تدريبهم على إطلاع ذويهم على كلِّ ما يرونه على الإنترنت، وتدريبهم على كَيْفِيَّةِ التَّعَامُلِ مع بعض المواقع، كالتَّسَمُّرِ عبر الإنترنت، فعند التَّعَرُّضِ للتَّسَمُّرِ عبر الإنترنت لا بُدَّ من تَوْعِيَةِ الطِّفْلِ بضرورة إخبار أهله أو مُعَلِّمِهِ في الصَّفِّ على الفور، وألاَّ يتجاوب مع المُتَسَمِّرِ وألاَّ يُنْفِذَ له أيَّ طلب، وألاَّ يكثر بالتَّهْدِيدَاتِ.

- **حماية الطِّفْلِ من الإدمان الرِّقْمِيِّ:**

يُعَدُّ الإدمان الرِّقْمِيُّ من الأخطار الحادَّةِ التي يُواجهها الأطفال على الإنترنت. ويُقصد بالإدمان الرِّقْمِيُّ استخدام الطِّفْلِ الإنترنت لساعات طويلة يومياً، وهو ما يترك آثاراً سلبية عليه، مثل تراجع التَّحْصِيلِ العِلْمِيِّ، وتراجع الفاعليَّةِ الاجتماعيَّةِ، ومَخَاطِرِ التَّعَرُّضِ للاكتئاب والسَّمَةِ وبعض الأمراض النَّفْسِيَّةِ والجسديَّةِ، وتراجع علاقته بأفراد أُسْرَتِهِ وبأصدقائه، لذلك وللحماية من مَخَاطِرِ الإدمان الرِّقْمِيِّ لا بُدَّ من تنظيم وقت الطِّفْلِ على الإنترنت، وأن يكون استخدامه له تحت إشراف مُباشِرٍ من الأهل.

- **تدريب الطُّفل على أساسيّات الاستخدام الآمن للإنترنت:**

من الضروريّ تدريب وتوعية الطُّفل بالأخطار الرّقميّة التي تتناسب مع عُمره، وتدريبه وتأهيله على كميّة الوقاية من هذه المخاطر، لا سيّما مخاطر التّمر عبر الإنترنت، وكميّة حماية البيانات الشخصيّة، وقواعد كتابة كلمات المرور.

أُسُس حماية الشَّباب من المَخاطر الرِّقْمِيَّة

هناك عددٌ من الأسُس والقواعد التي يمكن أن تُساعد في حماية الشَّباب من المَخاطر الرِّقْمِيَّة، خاصَّةً أنَّهم الشَّريحة الاجتماعيَّة الأكثر استخدامًا للإنترنت، والأكثر تعرُّضًا للمَخاطر الرِّقْمِيَّة. وفيما يلي تبيان لأهمِّ هذه الأسُس:

• التَّوجِيه والتَّوعِيَة:

لا بُدَّ من توعية الشَّباب بأساسيَّات الأمن السيبرانيِّ والسَّلامة الرِّقْمِيَّة، مثل ضرورة غَلْق الحسابات التي لا يتمُّ استخدامها على مواقع التَّواصل الاجتماعيِّ وغيرها؛ وذلك حتى لا تكون ثَغْرَة في الوصول إلى معلومات عنهم وعن حساباتهم المُستخدَمة، فغَلْق تلك الحسابات من عوامل الحماية المُهمَّة، مع ضرورة التَّوجِيه أيضًا إلى أهمِّيَّة حَذْف الأشخاص الذين لا يوجد معهم تَواصُل أو معرفة حقيقيَّة؛ لأنَّ ذلك يُسهم أكثر في تأمين الحسابات الخاصَّة بالشَّباب.

• دَمْج طُرُق الحماية الرِّقْمِيَّة في المناهج التَّعليميَّة:

وهي تلك التي يقوم الشَّباب بدراستها في المجالات كافَّة؛ بحيث تكون إحدى الموادِّ الأساسيَّة المُتضمَّنة في الدِّراسة، وذلك بما يتناسب مع سنِّ الدَّارس وقُدْرته على استيعاب تلك المعلومات، مع الحرص على تنمية فكرة اعتبار الإنترنت من وسائل التَّعليم والدَّعم وإيجاد الفُرص، وليس من وسائل التَّسليَة فقط؛ وذلك من أجل تقليل مُعدَّلات الاستخدام، وبالتالي تقليل مُعدَّلات الخطر، والعمل أيضًا على تنمية مهارات أخرى لدى الشَّباب، كممارسة الرياضة والقراءة.

- **تفعيل نظام إلكتروني للشكاوى:**

والتعريف بطرق تقديم الشكاوى؛ بحيث يتسنى للشباب الاستعانة بالمختصين في حال تعرضهم لمشكلات أو هجمات إلكترونية.

- **تفعيل سبل التوعية الرقمية من خلال المنصات الرسمية:**

ونشر فيديوهات توضيحية لطرق التعامل الرقمي الآمن، ونشر بعض التعليمات التي يجب على الشباب تجنبها أثناء التعامل الإلكتروني، مما يضمن بيئة رقمية أكثر أمانًا.

• التّدريب على قواعد الاستخدام الآمن للإنترنت:

في مرحلة الشّباب تزداد حدّة المخاطر الرّقمية مقارنةً بمرحلة الطّفولة، لذلك لا بُدّ من التّوسّع في مجال التّأهيل والتّدريب الرّقميّ، والتركيز على قواعد الاستخدام الآمن للإنترنت، بما يشمل كميّة إعدادات الخصوصية على البريد الإلكترونيّ ومواقع التّواصل الاجتماعيّ، وتفعيل مِيزة التّحقّق بخطوتين، والتي تشمل الحماية باستخدام معيارين للحماية، مثل استخدام كلمة المرور واستخدام بَصمة اليد في الوقت ذاته. إضافةً للتعريف بأهمّ الهجمات الإلكترونيّة، مثل هجوم برمجيات الفدية وحصان طروادة، وهجمات التّنصّت الوسيط وغيرها من الهجمات، وأسس الحماية منها، والحماية من هذه المخاطر تعتمد بشكلٍ رئيسٍ على اتّباع قواعد الاستخدام الآمن للإنترنت، بما يشمل كتابة كلمات مرور قويّة وتحميل البرامج والتّطبيقات من المواقع الرّسمية الموثوقة، والتّسوّق الإلكترونيّ عن طريق المتاجر الإلكترونيّة المعروفة، وعدم فتح مُرفقات البريد الإلكترونيّ الواردة من مَجْهولين، والتّدريب على مفاهيم سياسة أمان المحتوى، ومفهوم روبوتات الشبكة العالميّة، وكيف أنّ هذه الروبوتات قد تكون ضارّة أو نافعة.

• التّدريب على أُسس التّعامل مع البيانات:

بما يشمل التّشفير والتّخزين التّقليديّ والتّخزين على السّحابة، وأسس حماية البيانات، وأسس نقل البيانات عبر الشبكة، وأهمّ المخاطر التي تتعرّض لها البيانات، مثل القرصنة والتّخريب والتّزييف، والمخاطر التي تتعرّض لها شبكات نقل البيانات، مثل هجمات التّنصّت الوسيط، وهجمات منع الخدمة، وغيرها من المخاطر.

• توعية الشباب بالمخاطر السلوكية والنفسية للإنترنت:

لا بُدَّ من توعية الشباب بالآثار النفسية والسلوكية للإنترنت على حياتهم ومستقبلهم، فالإدمان الرقمي قد يؤدي لمشكلات نفسية وجسدية، كالانعزال الاجتماعي وضعف الثقة بالنفس وتراجع التحصيل العلمي، والقلق والاضطراب والأرق واضطرابات التغذية.

وعلى مستوى الآثار السلوكية فهي تشمل الميل للعنف والانفعال الزائد، والفتن، والتأثير السلبي على منظومة القيم الاجتماعية، لا سيما في حال التأثير بالثقافات الأخرى المختلفة عن الثقافات والعادات والتقاليد السائدة في المجتمع، إضافة لمخاطر المخدرات الإلكترونية، والقمار عبر الإنترنت، وإدمان الألعاب الإلكترونية، لذلك لا بُدَّ من توعية الشباب بكل هذه المخاطر.

أُسُس حماية الأسر من المخاطر الرقمية

الأسرة هي الجزء الأساسي المكوّن للمجتمع، وحماية الأسرة رقمياً تعني العمل على توعية رب الأسرة والمسؤول عنها، وكذلك الأمهات، بطرق التعامل الرقمي السليم؛ وبالتالي يكون الآباء مؤهلين رقمياً، وهو ما يساعد بشكل كبير على توعية أبنائهم وحمايتهم من المخاطر الرقمية المختلفة، وإن توعية الأسرة لها دور أساسي في تحقيق مجتمع رقمي آمن، فكما أنه من الأهمية بمكان تأهيل المعلمين رقمياً، لا بُدّ من تأهيل الوالدين رقمياً أيضاً.

ومن أهم الأسس التي يجب اتباعها لحماية الأسر من المخاطر الرقمية هو العمل على تدريب الآباء على التقنيات الحديثة والوسائل التكنولوجية المختلفة، والعمل على محو الأمية الرقمية لديهم؛ لأنّ الواقع الإلكتروني والتطورات المستمرة أصبحت تفرض نفسها، ولا بُدّ من تدريب الآباء على التعامل مع البيئة الرقمية؛ حتى يكون لديهم القدرة على توعية أبنائهم.

ويمكن تحقيق ذلك من خلال قيام مؤسسات المجتمع المدني والمؤسسات الحكومية بمختلف أنواعها بتقديم ورش ودورات تدريبية للموظفين؛ كونهم آباء أو حتى من الموظفين غير المتزوجين؛ لتزويد معلوماتهم الرقمية وتعريفهم بطرق الحماية من الهجمات والمخاطر الرقمية المختلفة، ولتعميم التجربة على كل الأسر.

أصبح تدريب الأسر على طُرُق الاستفادة من الخدمات الرّقمية أمرًا في غاية الأهميّة؛ حيث يمكنهم توجيه أبنائهم للاستفادة من هذه الخدمات، وبالتالي تعليمهم طُرُق الاستفادة الصّحيحة من الإنترنت، وتدريب الأسر أيضًا على طُرُق الحصول على المعلومات بشكلٍ آمن عبر الإنترنت، وطُرُق البحث الصّحيح عن المعلومات، وطُرُق التّعامل مع المعلومات وتصنيفها بشكلٍ مُناسب.

هذه الاستراتيجيّات يمكن أن تتبنّاها الدّولة بشكلٍ عامّ لتفعيل دور الأسرة في الاستخدام الآمن للإنترنت، وتأهيل الآباء للتعامل الرّقميّ الصّحيح، والقُدرة على توظيف التّكنولوجيا لخدمة الأسرة، وكذلك القُدرة على حماية الأبناء من المخاطر الرّقمية المختلفة.

كيف تحمي عائلتك من مخاطر الإنترنت؟

بات الإنترنت جزءًا رئيسًا من الحياة اليومية للأفراد والأسر، فالتعليم والخدمات الحكومية والترفيه والعمل، بات جزء كبير منه يتم عن طريق الإنترنت، وهذا ما يجعل الأسر في مواجهة تهديدات رقمية متصاعدة، الأمر الذي يحتم ضرورة الاهتمام بمواجهة التهديدات الرقمية، وذلك من خلال عدة سياسات وإجراءات، على رأسها اتباع قواعد التصفح الآمن للإنترنت، وهذه القواعد تُعد بمثابة درع حماية للفرد عند تعامله مع الإنترنت، وبشكل عام، يمكن وضع بعض القواعد التي تحمي الفرد والأسرة عند التعامل مع الإنترنت والأدوات التكنولوجية، وفيما يلي تبيان لأهم هذه القواعد.

• عدم الإفراط في مشاركة المعلومات الشخصية عبر الإنترنت

فمشاركة المعلومات الشخصية عبر الإنترنت قد يكون سببًا لتعرض الحسابات الشخصية للخرق، كما قد يؤدي للتعرض للتتبع عبر الإنترنت والتتبع الاحتيالي، والاحتيال عبر الإنترنت، وغيرها من المخاطر الرقمية، وتشمل المعلومات الشخصية أرقام الهواتف والصور العائلية وعنوان السكن ومكان العمل، وأسماء أفراد الأسرة، وتفاصيل الحياة الشخصية، وغيرها من المعلومات التي لا يجوز مشاركتها وإطلاع الآخرين عليها.

- **الاهتمام بكتابة كلمات مرور قوية وتغييرها بين الحين والآخر**

تُعَدّ كلمات المرور خطّ الدّفاع الأوّل ضدّ الهجمات الإلكترونيّة، لذلك لا بُدّ من الاهتمام بكتابة كلمات مرور قويّة، تشمل حروفًا صغيرة وكبيرة وأرقامًا ورموزًا، وألا تقل عن 12 حرفًا، والعمل على تغييرها بانتظام، إضافةً لضرورة الانتباه لعدم استخدام كلمة مرور واحدة لكلّ الحسابات، فلنّ حساب كلمة مرور خاصّة به.

كما لا يجوز مُشاركة كلمات المرور مع أيّ شخصٍ كان، وضرورة تجنّب وُضع كلمة المرور واسم المُستخدم في مكانٍ واحدٍ.

- **عدم استخدام شبكة WiFi عامّة**

في الوقت الرّاهن باتت شبكات الإنترنت WiFi المجانيّة متاحة في أماكن عدّة، كالمطاعم والمقاهي والمطارات والجامعات وغيرها من الأماكن، واستخدام الشّبكات العامّة المفتوحة قد يكون سببًا لتعرّضك لهجوم إلكترونيّ، مثل سرقة كلمات المرور أو خرق هاتفك المحمول وسرقة بياناتك الشخصيّة، وتعرّضك لهجمات البرمجيات الضّارة، وغيرها من المخاطر، لذلك يُفضّل عدم استخدام هذه الشّبكات المفتوحة، لا سيّما عند القيام بالعمليّات الماليّة، كدفع فاتورة أو عمليّة شراء عن طريق الإنترنت.

- **تثبيت برامج فحص الفيروسات والبرمجيات الضارة وتحديثها باستمرار**

تُعدّ البرمجيات الضارة والفيروسات من أبرز التهديدات الرقمية التي تواجه مستخدمي الإنترنت، خاصةً أنّ الخسائر الناجمة عن هجوم البرمجيات الضارة غالبًا ما يفتقرن بخسائر حادة، قد تكون خسائر مالية أو سرقة بيانات شخصية، أو التعرّض لهجوم الفدية، لذلك ولمواجهة هذه التهديدات لا بُدّ من تثبيت برامج لفحص الفيروسات والبرمجيات الضارة، والعمل على تحديثها باستمرار.

- **ضرورة تحديث نظم التشغيل الخاصة بالحاسوب والهواتف المحمولة والأجهزة اللوحية**

تحديث نظم تشغيل الأجهزة الإلكترونية يُعدّ عاملاً رئيساً من عوامل الحماية والسلامة الرقمية، خاصةً أنّ النسخ الأحدث من نظم التشغيل تتضمن عوامل أمان إضافية، كما تكون مهيأة للتعامل مع التهديدات الرقمية الحديثة، لذلك لا بُدّ من متابعة الإصدارات الحديثة من نظم التشغيل، والعمل على تثبيتها فور ظهورها.

• اتّباع قواعد التّصفّح الآمن للإنترنت

إضافةً إلى ما سبق؛ فإنّ قواعد التّصفّح الآمن للإنترنت تحمي الفرد والأسرة من المخاطر الرّقمية والهجمات الإلكترونيّة، وتشمل هذه القواعد الأساس والاعتبارات التّالية:

- **عدم فتح المِلَفّات والرّوابط المرفّقة مع البريد الإلكترونيّ الوارد من شخص مجهول:** فهذه المرفّقات قد تحتوي على ملَفّات ضارّة أو برمجيات خبيثة؛ لذلك لا بُدّ من حذفها وعدم فتحها.

- **عدم الاستجابة للرسائل التي تتحدّث عن ربح مَبْلَغ ماليّ أو هاتف محمول:** فغالبية هذه الرّسائل تكون أداةً للتّصيّد الاحتياليّ، وتهدف لسرقة بياناتك الشّخصيّة، أو تطلب منك تحويل مبلغ ماليّ بسيط لحساب ما، وذلك بحجج مختلفة، قد تكون بحجّة تكاليف شحن الهدية، لذلك لا يجب تصديق هذه الرّسائل، ويجب حذفها فوراً، وعدم فتح أيّ رابط موجود بها.

- **عدم فتح الإعلانات المنبثقة في المواقع الإلكترونيّة:** في العديد من المواقع يجد المُستخدم أمامه مجموعة من الإعلانات، والتي تكون مُصمّمة بطريقة تجذب المُستخدم لفتح روابطها، وفي غالبية الأحيان تكون هذه الإعلانات أداةً للتّصيّد الاحتياليّ أو للاحتيال عبر الإنترنت، أو تكون مُتضمّنة برمجيات خبيثة، لذلك من الأفضل تجاهل هذه الإعلانات.

• **تحميل البرامج والتطبيقات والملفات من المواقع الرسمية الموثوقة:** توجد مئات وآلاف المواقع الإلكترونية التي تُقدّم خدمة تحميل البرامج والتطبيقات وملفات الفيديو والكُتب الإلكترونية، لكن هذه المواقع تُعدّ خَطرَة، بسبب أنّ البرامج المُحمّلة عن طريقها قد تكون مُلوّثة بِبرمَجِيّات خَطرَة.

• **عدم التسوّق الإلكتروني إلّا من خلال المتاجر المعروفة والموثوقة:** فحاليًا هناك عدد كبير من المتاجر الإلكترونية التي تُقدّم خدمات التسوّق الإلكتروني، لكنّ التعامل مع غالبيتها يُعدّ خطرًا، فهي غير موثوقة، فقد يتمّ من خلالها سرقة معلومات بطاقات الدّفع، وبالتالي سرقة الرّصيد في البطاقة، أو قد تكون مَدْخَلًا لِلتَّعَرُّض للاحتيال عبر الإنترنت، لذلك يُفَضَّل حَصْر التسوّق الإلكتروني بالمواقع المشهورة والموثوقة.

• **ضرورة الاحتفاظ بنسخ احتياطية للبيانات المهمّة:** ففي حال التّعرُّض لهجوم إلكتروني قد تتلف البيانات المُخزّنة على الجهاز المُستَهدَف، لذلك لا بُدّ من الاحتفاظ بنسخ احتياطية على السّحابة أو على أداة تخزين خارجيٍّ مثل قُرْص صلب خارجيٍّ غير مُتّصل بالإنترنت.

ختامًا لهذا الدليل، لا بُدَّ من التأكيد بأنّه وعلى الرغم من الارتفاع الحادّ في مُعدّل الهجمات الإلكترونيّة التي تتعرّض لها مختلف شرائح المجتمع؛ إلّا أنّ الوقاية من هذه المَخاطر مُمكن وبسيط، ويعتمد بشكلٍ رئيسٍ على الوَعْي بهذه المَخاطر، وعلى الوَعْي بقواعد التّصفّح الآمن للإنترنت، واستخدام الإنترنت بانتظام وضمن ضوابط مُحدّدة؛ منعًا من التّعرّض لمَخاطر الإدمان الرّقميّ.

المراجع



أولاً: الكتب والدوريات

1. أحمد السيّد، محمود عليّ، الإفراط في استخدام الإنترنت وبعض مُتغيّرات الشّخصيّة لدى طلاب الجامعة، مجلة دراسات عربية في التّربية وعلم النفس، المجلد رقم 3، العدد 2، مصر، 2009م، ص 182، 183.
2. أحمد عيسى نعمة، الفتلاوي، الهجمات السيبرانيّة: مفهومها والمسؤوليّة الدوليّة الناشئة عنها في ضوء التّظيم الدوليّ المعاصر، مجلة المحقّق الحليّ للعلوم القانونيّة والسياسيّة، العدد الأوّل، المجلد 44، 2020م، ص 49 - 76.
3. دحماني، سليم، "أثر التّهديدات السيبرانيّة على الأمن القوميّ.. الولايات المتّحدة الأمريكيّة أنموذجاً، 2001-2017م"، جامعة محمد بوضياف المسيلة، قسم العلوم السياسيّة، 2018م.
4. رحمين، نهاد، عتيقة كواشي، مقارنة التّمكن المعلوماتيّ للمرأة: حماية الطّفل من مخاطر المعلوماتيّة، مجلة الإحياء، المجلد 22، العدد 31، 2022م، ص 687.
5. سعيد محمود، آمال محمد، مخاطر المُخدّرات الرّقميّة على الشّباب الجامعيّ ودور خدمة الجماعة في التّخفيف منها، مجلة جامعة أسوان للعلوم الإنسانيّة، المجلد الثاني، العدد 2، مصر، 2022م، ص 96، 97.

-
6. الشطري، حامد مجيد فارة، الإدمان الرقمي وعلاقته بالعزلة الاجتماعية لدى طفل طيف التوحد من وجهة نظر أولياء أمورهم، مجلة الباحث الإعلامي، العدد 56، كلية الإعلام، جامعة بغداد، العراق، ص 44، 45.
7. العراقي، صالح، تعرّض الشباب الجامعي المصري للمواقع الإلكترونية التي تهتمّ بقضايا المخدرات وعلاقته بإدراكهم لمخاطر إدمان المخدرات الرقمية، المجلة العلمية لبحوث الإذاعة والتلفزيون، العدد 11، مصر، ص 124.
8. فرحات، علاء الدين، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الثالث، 2019م.
9. كمال، محمد، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلاً من القنبلة، دار كلیم للطباعة والنشر والتوزيع (القاهرة - مصر)، ط 1، 2022م، ص 11.
10. محمد حسين، سارة، إجراءات مقترحة لإدارة المخاطر السيبرانية، مجلة الإدارة التربوية، العدد الرابع والثلاثون، أبريل 2022م، ص 349.
11. موجز السياسة العامة للحفاظ على سلامة الأطفال في البيئة الرقمية، الاتحاد الدولي للاتصالات، 2021م.

ثانيًا: المراجع الإلكترونيّة

1. أبرز سبعة مخاطر يُواجهها الأطفال على الإنترنت: كيفية الحفاظ على أمنهم، kaspersky، مُتاح على الرابط: <https://me.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online>
2. أكثر من 175,000 طفل يستخدمون الإنترنت للمرّة الأولى كلّ يوم، مستفيدين من فُرص كبيرة، ولكنهم يُعرضون أنفسهم لمخاطر جسيمة، الموقع الرّسمي لمنظمة الأمم المتّحدة، 6 فبراير 2018م، مُتاح على الرابط: <https://www.unicef.org/ar/البيانات-الصحفية/أكثر-من-175000-طفل-يستخدمون-الإنترنت-للمرة-الأولى-معرضين-مخاطر>
3. الأمن السيبرانيّ خلال كأس العالم: الجهود تتواصل لضمان فضاء سيبرانيّ مفتوح وآمن في دولة قطر، مركز قطر للتّطوير المهنيّ، مُتاح على الرابط: <https://qcdc.org.qa/ar/fifa/الأمن-السيبراني-خلال-كأس-العالم-الجهو/>
4. جرائم الإنترنت تزحف لعالمنا الحقيقي. والاستعباد الإلكترونيّ يأسر الآلاف، CNN، مُتاح على الرابط: <https://cnnbusinessarabic.com/technology/43132/جرائم-الإنترنت-تزحف-لعالمنا-الحقيقي-والاستعباد-الإلكتروني-يأسر-الآلاف>
5. سياسة إدارة البيانات، وزارة الاتّصالات وتكنولوجيا المعلومات، دولة قطر، 2015م، مُتاح على الرابط: <https://www.mcit.gov.qa/ar/documents/document/data-management-policy>

-
6. قطر الأولى عالميًا في سرعة إنترنت الهاتف الجوال وفي استخدام شبكة الإنترنت، وكالة الأنباء القطريّة، 9 مارس 2021م، مُتاح على الرابط: <https://www.qna.org.qa/ar-QA/News-Area/News/2021-09/03-0058-قطر-الأولى-عالميا-في-سرعة-إنترنت-الهاتف-الجوال-وفي-استخدام-شبكة-الإنترنت>
7. المُتاجرون بالبشر يجدون ضحاياهم عبر مواقع التّواصل الاجتماعيّ وألعاب الفيديو، الموقع الرّسميّ لمنظمة الأمم المتّحدة، 21 أكتوبر 2021م، متاح على الرابط: <https://news.un.org/1085552/10/ar/story/2021>
8. الهجمات الإلكترونيّة (السّبيرانيّة) والتّأمين، نشرة الاتّحاد المصريّ للتّأمين، عدد رقم 67، لعام 2019م، مُتاح على الرابط: <https://cutt.us/gHPNu>
9. اليونيسف: لتجّقل العالم الرّقميّ أكثر أمانًا للأطفال- مع زيادة الوصول إلى الإنترنت لتحقيق الفائدة للفئات الأكثر حرمانًا، الموقع الرّسميّ لمنظمة اليونيسف، 11 ديسمبر 2017م، مُتاح على الرابط: <https://www.unicef.org/ar/البيانات-الصحفية/الانترنت-لتحقيق-الفائدة-للفئات-الأكثر-حرمانًا>

ثالثاً: المراجع الأجنبية

1. An Introduction to Information Security, Michael Nieves&Victoria Yan Pillitteri& Kelley Dempsey, June 2017, National Institute of Standard and Technology, U.S.Department of Commerce.
2. Andy Herman, MSIM, CISSP, Security and Infrastructure Intern West Monroe Partners, LinkedIn, 5 Jul 2016, on site: <https://www.linkedin.com/pulse/importance-cybersecurity-understanding-preventive-medicine-herman/>
3. Cyberattacks on young gamers up 57 percent in 2022, Kaspersky, on site: https://www.kaspersky.com/about/press-releases/2023_cyberattacks-on-young-gamers-up-57-percent-in-2022
4. Data Security Breach: 5 Consequences for Your Business, The Am Group, on site: <https://www.theamegroup.com/security-breach/>
5. Growing Up in a Connected World, UNICEF, 2020, on site: <https://www.unicef-irc.org/growing-up-connected>
6. Growing Up in a Connected World, UNICEF, 2020, on site: <https://www.unicef-irc.org/growing-up-connected>

-
7. How Conti ransomware hacked and encrypted the Costa Rican government, bleeping computer, on site: <https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/>
 8. Internet Safety for Kids & Teens, Chapter 1: Cyber Threats to Kids & Teens, on site: <https://codesigningstore.com/cyber-threats-to-kids-and-teens>
 9. Internet Safety for Kids & Teens, Chapter 1: Cyber Threats to Kids & Teens, on site: <https://codesigningstore.com/cyber-threats-to-kids-and-teens>
 10. Kovacs, Eduard. Cybercrime Losses Exceeded \$10 Billion in 2022, security week, 13 March 2023, on site: <https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/>
 11. Kumar, G., Kameshwari, L. and Gunjan, V.K. (2021) Malware Techniques and Its Effect: A Survey, research gate, on site: https://www.researchgate.net/publication/360615209_Malware_Techniques_and_Its_Effect_A_Survey.
 12. Lehto Martti, Neittaanmäk Pekka Cyber Security: Analytics, Technology and Automation Switzerland: Springer International Publishing, 2015.

-
13. Lydon, Mark. 11 Companies Who Have Recently Faced a Cyberattack, Auto Grow, on site: <https://www.autogrow.co/recent-cyber-attacks-on-companies/>
 14. NCHampson, "Hacktivism: A new breed of protest in a networked world" BC Int'l & Compl Revvol35, p511, 2012
 15. Nivedita James, 51 Small Business Cyber Attack Statistics 2023 (And What You Can Do About Them), September 2023, on site: <https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/>
 16. out of 10 children exposed to cyber risks online, study finds, TRT world, 2021, on site: <https://www.trtworld.com/magazine/6-out-of-10-children-exposed-to-cyber-risks-online-study-finds-56733>
 17. Sanborn Colaco, How Can Educational Institutions Mitigate Cybersecurity Threats in Education? kitaboo, 18 Jul2023, on site: <https://kitaboo.com/how-educational-institutions-mitigate-cybersecurity-threats-in-education/>
 18. Steve Morgan, 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics, Cybercrime magazine, published at: <https://cybersecurityventures.com/cybersecurity-almanac-2023/>.

-
19. Steve Morgan, Editor-in-Chief, Cybercrime to Cost The World \$10.5 Trillion Annually By 2025, cybersecurity ventures, 13 Nov 2020, on site: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
 20. Steve Morgan, previous reference available at: <https://cybersecurityventures.com/cybersecurity-almanac-2023/>.
 21. The Latest 2023 Cyber Crime Statistics (updated August 2023), available at: <https://aag-it.com/the-latest-cyber-crime-statistics/>
 22. The Latest 2023 Cyber Crime Statistics (updated October 2023), AAG, 2 October 2023, on site: <https://aag-it.com/the-latest-cyber-crime-statistics/>
 23. The Latest 2023 Cyber Crime Statistics (updated October 2023), AAG, 2 October 2023, on site: <https://aag-it.com/the-latest-cyber-crime-statistics/>
 24. The Top 10 Countries Most Targeted by Cyberattacks, blogs, 2023, on site: <https://blogs.blackberry.com/en/202302/top-10-countries-most-targeted-by-cyberattacks-2023-report>

-
25. Toy firm VTech hack exposes private data of parents and children, The Guardian, 30 November 2015, on site: <https://www.theguardian.com/technology/2015/nov/30/vtech-toys-hack-private-data-parents-children>
26. United States Cybersecurity Market - Growth, Trends, COVID-19 Impact, and Forecasts (2023 - 2028), Mordor Intelligence, on site: <https://www.mordorintelligence.com/industry-reports/united-states-cybersecurity-market>
27. Valeriano, Brandon and CManess, Ryan: «international relations theory and cyber security threats conflicts and ethics in an Emergent Domain in an emergent domain» in The Oxford Handbook of International Political Theory, edited by Brown Chris and Eckersley Robyn United Kingdom: Oxford University Press
28. What is a Computer Virus or a Computer Worm? Kaspersky, <https://me-en.kaspersky.com/resource-center/threats/viruses-worms>.
29. What is Cyber Security? Kaspersky, on site: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>

-
30. What is Ransomware Attack? Imperva, on site: <https://www.imperva.com/learn/application-security/ransomware>.
31. What Is Ransomware? Proofpoint, on site: <https://www.proofpoint.com/us/threat-reference/ransomware>.
32. What is Spyware? Kaspersky, on site: <https://www.kaspersky.com/resource-center/threats/spyware>.
33. Ybarra, MLLinkages between Depressive Symptomatology and Internet Harassment among Young Regular Internet UsersCyber Psychology and Behavior, (2), (2007)247- 257.

