CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

مَخاطِر الأَمْن السّيبرانيّ

حَقِيبة تدريبيَّة

خاصَّة بالمُدَرِّب

المرحلة الابتدائيَّة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مَخاطِر الأَمْن السّيبرانيّ

المرحلة الابتدائيَّة

حَقِيبة تدريبيَّة خاصَّة بالمُدَرِّب

حُقُوق المِلْكِيَّة الفِكْرِيَّة

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

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

المحتوى العام للحقيبة

أولاً: مدخل عام للحقيبة

ثانياً: المادة العلمية

أولًا: مَدْخل عامّ إلى الحَقيبَة التَّدْريبيَّة

فيما يلي تبيان لبعض التَّفاصيل ذات الصِّلَة المُباشِرَة بأهداف الحَقيبَة التَّدْريبيَّة، مع توجيهات عامَّة للمُدَرِّب حول كيفيَّة التَّعامُل مع هذه الحَقيبَة، وتزويده بالمحتوى العِلْميّ الذي سيَعْتَمِد عليه في التَّدريب.

الفكرة العامَّة

تقوم فكرة هذه الحَقيبَة التَّدْريبيَّة على تزويد المُدَرِّب بأدوات ووسائل تدريبيَّة؛ بحيث يسهل عليه تقديم المعلومات للمُتَدَرِّبين. وبشكلٍ عامّ فإنَّ المادة التَّدريبيَّة تكون على جُزأين؛ جُزء لدى المُتَدَرِّب وجزء آخر لدى المُدَرِّب، والحَقيبَة التَّدْريبيَّة تُعدّ بمثابة مُوجِّه عامّ للمُدَرِّب وداعِم له، ومحتواها العِلْميّ هو ذاته لدى المُتَدَرِّب، ولكنْ بأسلوب عَرْض مُختَلف؛ إضافةً إلى تزويد المُدَرِّب بأدواتٍ ووسائل تدريب تَدْعَمه في عمليَّة التَّدريب.

أهداف الحَقيبَة التَّدْريبيَّة

- تَزويد المُدَرِّب بوسائل تدريب تُساعده على إيصال المحتوى التَّدريبيّ للطَّلبة.
- تَقديم المعلومات والمحتوى التَّدريبيّ بشكلٍ سَهْل ومُبسَّط.
- تَقْديم المحتوى التَّدريبيّ الخاصّ بمَخاطِر الأَمْن السّيبرانيّ مرفقًا بأدوات ووسائل تدريب مُتَعَدِّدَة.

محتوى الحَقيبَة التَّدْريبيَّة

تتضمَّن الحَقيبَة التَّدْريبيَّة عدَّة أدوات تدريبيَّة، فيما يلي تبيان لها:

1. **ملفّ العَرْض.**
2. **ألعاب تدريبيَّة،** كتلوين الأشكال، يقوم المُدَرِّب بعَرْضها على الطُّلاب؛ بهدف ضمان تَفاعُلهم مع المحتوى التَّدريبيّ.
3. **فيديوهات تَعليميَّة.**
4. **مُسابَقات،** وهي على شَكْل أسئلة استنتاجيَّة يَعْرضها المُدَرِّب على الطَّلبة بهدف التَّفاعُل فيما بينهم.
5. **بطاقات تدريبيَّة،** وهي على شَكْل معلومات عامَّة مُرفَقَة بصُوَر تعبيريَّة، يَعْرضها المُدَرِّب على الطَّلبة.
6. **إسكتشات،** تتضمَّن معلومات حول المحاور الرَّئيسة في المحتوى التَّدريبيّ.

فهرس المحتوى العِلْمِيّ

الفَصْل الأَوَّل
مفهوم الأَمْن السّيبرانيّ والسَّلامَة الرَّقميَّة

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تمهيد	5 دقائق
الجُزْء النَّظريّ من المادَّة	25 دقيقة
عَرْض الفيديوهات التَّعليميَّة	25 دقيقة
استراحة قصيرة	20 دقيقة
تنفيذ الأَلْعَاب التَّدريبيَّة	25 دقيقة
حِوَار ونِقَاش مع الطَّلَبة	15 دقيقة
مَشروع التَّخرُّج	5 دقائق
المُدَّة الزَّمنيَّة للورشَة	ساعتان

دليل إرشادي للمُدَرِّب

فيما يلي تبيان لبعض الإرشادات العامَّة للمُدَرِّب، والتي تتمحور حول كيفيَّة استخدام هذه الحَقيبَة.

1. المحتوى العِلْمِيّ للحَقيبَة قد يَفُوق قُدْرة الطَّلبة على الاستيعاب؛ خاصَّةً من ناحية المصطلحات والمفاهيم العامَّة؛ لذلك لا بُدَّ للمُدَرِّب أن يقوم بتبسيط هذه المفاهيم وتقديمها بصورةٍ قابلةٍ للفَهْم مِن قِبَل طلبة المرحلة الابتدائيَّة.
2. يقوم المُدَرِّب بعَرْض شرائح العَرْض عند كُلّ نقطة يتحدَّث عنها، فمثلًا عند الحديث عن الأَمْن السّيبرانيّ يَتمّ عَرْض الشَّريحة الأُولى: ما هو الأَمْن السّيبرانيّ؟
3. عَقب شرح الفصلين الأوَّل والثَّاني من المادَّة العِلْمِيَّة يَتمّ إعطاء اختبار بسيط لهم هو "ضع علامة (√) أو علامة (X) أمام كُلّ جُمْلَة".
4. في أثناء شرح الفَصْل الأَوَّل يَتمّ توزيع الصُّوَر المُصمَّمة خِصِّيصًا لفقرة "هل تعلم؟"
5. يَعرِض المُدَرِّب الجزء الخاص بـ "إسكتشات" في أثناء قيام الطَّلبة بحل التَّمارين والتَّدريبات.
6. في نهاية التَّدريب يَتمّ عَرْض أسئلة المسابقات المذكورة في نهاية الملفّ.
7. في أثناء عرض المادَّة العِلْمِيَّة لكلّ فَصْل يَتمّ استقطاع فترة من الوقت المُخصَّص له لعَرْض عددٍ من الرَّوَابِط ذات الصِّلَة بمضمون الفصل.
8. يقوم المدرب بعرض الفيديوهات التعليمية -المذكورة في ملف منفصل- على الطَّلبة في نهاية كل فصل، أو في الموضع الذي يراه مناسبًا.
9. ذِكْر أمثلة على حوادث سيبرانيَّة حدثت خلال عرض المادَّة العِلْمِيَّة.
10. عند طَرْح سؤال: "كيف يمكننا تمييز الفَرْق بين المِزَاح وبين التَّنَمُّر عبر الإنترنت؟" يُرْجَى فَتْح باب النِّقاش مع الطَّلبة للاستماع إلى آرائهم.
11. فيما يخصُّ التَّمارين المُوجَّهة للطَّلبة؛ سيتمّ إرفاق ملفّ بالتَّمارين في نهاية هذه الحَقيبَة، وهذه التَّمارين تُقسَّم لجزأين؛ جُزْء يتمّ تقديمه للطَّلبة خلال التَّدريب، وهو تمارين صَفِّيَّة، والجزء الآخر يُكلَّف الطَّلبة بالإجابة عنه في المنزل، وهو تمارين لا صَفِّيَّة، وسيتمّ توضيح هذه الجزئيَّة في نهاية هذه الحقيبة.

مشروع التَّخرُّج

مشروع التَّخرُّج هو عملٌ يَقُوم به الطَّالب، ويهدف لتحقيق عدَّة أهداف، فيما يلي تبيان لأهمّها:

- التَّأكُّد أنَّ الطَّالب قد استوعَب المعلومات والأفكار التي تمَّ تقديمها له، وأنَّه بات قادرًا على الاستفادة منها في حياته اليوميَّة.
- ترسيخ المعلومات والأفكار التي تمَّ تقديمها للطَّالب.
- المشروع بمثابة رَبْط للأفكار والمعلومات النَّظريَّة بالواقع العَمَليّ والتَّطبيقيّ.

فيما يَتعلَّق بآليَّة تكليف الطَّلبة بالمشروع، وكيفيَّة تنفيذه، يمكن تقديم التَّوجيهات التَّالية:

- يمكن أن يكون مشروع التَّخرُّج فَرْديًّا أو جَماعيًّا، وفي حال كان جَماعيًّا يجب ألَّا يَتجاوز عدد الطَّلبة المشتركين في مشروعٍ واحدٍ ثلاثة طَّلبة.
- اختيار موضوع المشروع يكون مِن قِبَل الطَّلبة، ويمكن للمُدَرِّب تقديم بعض المُساعَدة أو الأفكار في هذا المجال، والمشروعات الخاصَّة بطلبة الصُّفوف الأوَّل والثَّاني والثَّالث تكون بإشرافٍ مُباشِر مِن قِبَل المُدَرِّب، أمَّا مشروعات طلبة الصُّفوف الرَّابع والخامس والسَّادس فتكون بإشراف غير مُباشِر منه.
- موضوع مشروع التَّخرُّج لا بُدّ أن يكون مُنسجمًا مع المحتوى التَّدريبيّ الذي تمَّ تقديمه للطَّلبة.
- يمكن أن يكون مشروع التَّخرُّج ضِمْن أحد التَّصوُّرَات التَّالية، وهي تَصوُّرَات غير مُلْزِمَة، فيمكن للمُدَرِّب اختيار تَصوُّرَات أخرى يراها مُناسِبَة، وفيما يلي تبيان لبعض المُقْتَرَحَات:
  - كتابة قِصَّة قصيرة تَدُور أحداثها حول طِفْل تَعرَّض لخطرٍ أو هجومٍ رقميّ؛ كقَرْصنة بياناته مثلًا، وكيف تَصرَّف حِيَال هذا الموقف.
  - يَتَقَمَّص الطَّالب دَوْر المُدَرِّب ويَكْتُب تَوْجِيهاتٍ عامَّةً لزملائه أو أَهْله يُوضِّح لهم فيها الإجراءات المطلوبة للوقاية من المَخَاطِر الرَّقميَّة.

ثانيًا: المادَّة العِلْمِيَّة

الفَصْل الأَوَّل

مفهوم الأَمْن السّيبرانيّ والسَّلامَة الرَّقميَّة

- مفهوم الأَمْن السّيبرانيّ
- خصائص ومهامّ الأَمْن السّيبرانيّ
- الفَرْق بين الأَمْن المَعْلُومَاتيّ والأَمْن السّيبرانيّ

01

أولًا: مفهوم الأَمْن السّيبرانيّ

ما هو الأَمْن السّيبرانيّ؟

هو حماية الشَّبكات وأنظمة تقنيّات المعلومات وأنظمة التِّقنيات التَّشْغيليَّة، ومُكوّناتها من أجهزة وبرامج، وما تُقدِّمه من خِدْمَات، وما تَحتويه من بيانات، من أيّ خرق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأَمْن السّيبرانيّ: أَمْن المعلومات، والأَمْن الإلكترونيّ، والأَمْن الرَّقميّ، ونحو ذلك. والأَمْن السّيبرانيّ هو عبارة عن مجموعة من الوسائل التِّقنية والإداريَّة والتَّنظيميَّة التي يَتمّ الاعتماد عليها واستخدامها لمَنْع سرقة المعلومات الإلكترونيَّة للأفراد والمُؤسَّسَات، كما يساعد على استعادة كافَّة المعلومات التي تمَّت سرقتها[1].

أهميَّة الأَمْن السّيبرانيّ

نظرًا لاتِّجاه العديد من دُوَل العالَم إلى التَّحَوُّل الرَّقميّ في كثيرٍ من القطاعات، وظهور ما يُسمَّى بالاقتصاد الرَّقميّ والاستثمار في القطاعات التِّقنية، أوجَد ذلك حاجةً لحماية مَصَالح مُستخدِمي خِدْمَات الاتِّصالات وتقنية المعلومات.

ويُعدّ الأَمْن السّيبرانيّ من أهمّ الفروع الخاصَّة بالتّكنولوجيا التي تهدف إلى حماية كافَّة المعلومات المُهمَّة الخاصَّة بالأفراد والمُؤسَّسَات العامَّة والخاصَّة من الهجمات الإلكترونيَّة التي تُؤدّي إلى انتهاك خصوصيَّة المُؤسَّسَات أو حتى الأفراد.

لذلك بعد التَّقدُّم الكبير الذي حدَث في عالم التّكنولوجيا، وأيضًا مع تَطوُّر المُعَامَلات الرَّقميَّة المختلفة أصبح الاهتمام بالأمن السّيبرانيّ من القضايا بالغة الأهميَّة، ما يعني أنَّه يساعد على حماية الأفراد والمُؤسَّسَات من الهجمات الرَّقميَّة التي قد يَشنّها القراصنة عبر الإنترنت على كافَّة الأجهزة التي يَتمّ استخدامها بشكلٍ يَوْميّ مثل (أجهزة الحاسوب، الأجهزة الرَّقميَّة، الهواتف الذّكيَّة، الأجهزة اللَّوحيَّة). خاصَّةً مع ظهور أشكال وأدوات جديدة من الهجمات الإلكترونيَّة -في ظلّ التَّطوُّر التكنولوجيّ- تَستهدف بشكلٍ كبيرٍ سرقة كافَّة البيانات والمعلومات، وما يَتْبَع ذلك من الاحتيال وسرقة الأموال[2].

1. يوسف، أمير. (2015م). جرائم تقنية المعلومات بدُوَل الخليج العربيّ، والجهود الدّوليَّة والمحلّيَّة لمكافحته، جرائم الإنترنت والحاسوب الإلكترونيَّة في دُوَل الخليج العربيّ. مصر: دار الكتب العربية. ص -68 74.
2. المَرجع السَّابق.

أنواع الأَمْن السّيبرانيّ

هناك عدَّة أنواع مختلفة من الأَمْن السّيبرانيّ، وهي:

النَّوْع الأوَّل: أَمْن الشَّبكات Network Security

تَتـمّ أغلـب الهجمـات الإلكترونيَّـة مـن خـلال الشَّـبكات الإلكترونيَّـة، ومـن أفضـل الحلـول هنـا الاعتمـاد علـى الأَمْـن السّـيبرانيّ؛ لحمايـة كافَّـة شـبكات الحاسـوب مـن الهجمـات، فهنـا يسـاعد الأَمْـن السّـيبرانيّ علـى توفيـر أفضـل الحلـول الفَوْريَّـة للتَّحكُّـم الكامـل فـي عناصـر البيانـات والقُـدْرَة علـى الوصـول للشَّـبكات؛ لمَنْـع سـرقة البيانـات المُخزَّنـة، وغيرهـا.

النَّوع الثَّاني: الأَمْن السّحابيّ Cloud Security

فـي الفتـرة الأخيـرة تـمَّ الاعتمـاد علـى الـذَّكاء الاصطناعـيّ مِـن قِبَـل الأفـراد والمُؤسَّسَـات؛ بهـدف تحسـين جَـوْدَة العمـل، وإنجـاز الكثيـر مـن المهـامّ فـي أقـلّ وقـتٍ. ومـن المعـروف أنَّ كَـمّ البيانـات التـي يَتـمّ تخزينهـا مـن الصَّعْـب أن يَتـمّ الاحتفـاظ بهـا؛ لـذا هنـاك العديـد مـن الشَّـركات المختلفـة تعمـل علـى توفيـر أفضـل الخِدْمَـات التـي تسـاعد علـى حـلّ تلـك المشـكلة فـي وقـتٍ قياسـيّ، ومـن أفضـل تلـك الخِدْمَـات: Microsoft Azureg Google Cloud.

النَّوع الثَّالث: أَمْن التَّطبيقات

مـن المعـروف أنَّ تطبيقـات الويـب يَتـمّ اتِّصالهـا بالإنترنـت؛ ممَّـا يُعرِّضهـا لإمكانيَّـة الخـرق وسـرقة البيانـات. ويعمـل الأَمْـن السّـيبرانيّ علـى حمايـة البيانـات مـن أيّ هجمـات مثـل الفيروسـات وتَشْـفير المعلومـات، وغيرهـا.

النَّوع الرَّابع: الأَمْن التَّشْغيليّ

فـي حـال تعرُّض البيانـات إلـى الخـرق يساعد الأَمْـن السّـيبرانيّ علـى الوصـول إلـى العديـد مـن الخُطَـط البَديلَـة، ويظهـر هـذا النَّـوْع فـي أغلـب الشَّـركات والمُؤسَّسَـات الضَّخْمَـة[1].

1. yagibca, prateekt (2023) Cyber Security, types and importance, GeeksforGeeks. On site: https://www.geeksforgeeks.org/cyber security-types-and-importance/

ثانيًا: خصائص ومهامّ الأَمْن السّيبرانيّ

للأمن السّيبرانيّ العديد من المُمَيِّزات والفوائد نَضعها أمامكم في النِّقاط التّالية:

حماية البيانات

من المعروف أنَّ الهجمات الإلكترونيَّة تُسبِّب قلقًا كبيرًا للعديد من الشَّركات والمُؤسَّسَات؛ فقد تُؤدِّي إلى عدم قُدْرتها على حماية البيانات الخاصَّة بعملائها، ولكي تتمكَّن من الحِفَاظ على كافَّة بيانات العملاء وحمايتها لا بُدَّ من الاستعانة بأدوات الأَمْن السّيبرانيّ؛ للحفاظ على سرِّيَّة كافَّة البيانات.

حماية المِلْكِيَّة الفكريَّة

تُعدّ حماية المِلْكِيَّة الفكريَّة من أهمّ الجوانب الخاصَّة بالأَمْن السّيبرانيّ، وهناك أنواع خاصَّة بحماية المِلْكِيَّة مثل: العلامة التّجاريَّة، البيانات والأسرار الخاصَّة بالتّجارَة، حقوق النَّشْر، وغيرها.

الحماية من سرقة الأموال

عليك أنْ تعلم أنَّ هناك العديد من مُجْرمي الإنترنت يبحثون عن الثّغرَات التي يمكن من خلالها سرقة الأموال الخاصَّة بالمشروعات التّجاريَّة الصَّغيرة والكبيرة، وهنا تأتي الحاجة إلى تحديث البرامج واستخدام كلمات مرور قويَّة، وتشفير البيانات المُهمَّة.

الحماية من التَّجَسُّس

يساعد الأَمْن السّيبرانيّ في مَنْع مخترقي الأجهزة والبيانات من التَّجَسُّس على الأفراد والمُؤسَّسَات؛ حيث تُؤدِّي عمليَّات التَّجَسُّس إلى زيادة فُرَص سرقة البيانات الشَّخصيَّة وأرقام البطاقات الائتمانيَّة، والتي إن لم يكن عليها غطاء أمنيّ كافٍ يمكن خرق الأجهزة وسَرقتها.

زيادة ثقة العملاء

من الأمور التي يُحقِّقها الأَمْن السّيبرانيّ زيادة ثقة العملاء بالمؤسَّسات والشَّركات التي يتعاملون معها؛ حيث تُوفِّر الإجراءات الأمنيَّة المُعتمَدة -مثل: أنظمة الكشف والأنظمة الخاصَّة بمَنْع التَّطفُّل، بالإضافة إلى الأنظمة الخاصَّة بالتَّشْفِير- حمايةً عاليةً لبيانات العملاء السِّرِّيَّة.

حماية الأعمال

يساعد الأَمْن السّيبرانيّ في التَّصفُّح الآمن للإنترنت، ومُمارَسة العمل بشكلٍ آمِن دون الخوف من التَّهْديدات المُحتَمَلة التي يمكن أن تَحْدُث عَبْر شبكات الإنترنت.

حماية البيانات الشَّخصيَّة

يساعد الأَمْن السّيبرانيّ على حماية كافَّة البيانات الخاصَّة بالعملاء من السَّرِقَة أو التَّلاعُب بها، فخرق أيّ فيروس للأجهزة الإلكترونيَّة يعني وصول مخترقي الأجهزة والبيانات إلى جميع البيانات السِّرِّيَّة.

توفير الأمان والحِفَاظ على الإنتاجيَّة

عند خرق الفيروسات للأجهزة العَامِلة بالشَّركات والمُؤسَّسَات يَعُوق ذلك المُوظّفين عن أداء عملهم، وأحيانًا قد يتوقَّف العمل بالكامل، وهنا تبرز أهميَّة الأَمْن السّيبرانيّ؛ لمنع حدوث ذلك، أو التَّدخُّل فورًا في حال وقوع ذلك؛ لمَنْع تفاقُم المشكلة وعَوْدة العمل إلى طبيعته.

حماية المواقع الإلكترونيَّة

إذا كنتَ من مُتصفِّحي المواقع الإلكترونيَّة؛ عليك تذكُّر أنَّ عددًا كبيرًا من الشَّركات والمُؤسَّسَات وغيرها يمتلكون مواقع إلكترونيَّة لزيادة ثقة العُمَلاء بهم، وللحفاظ على سُمْعتهم الطَّيِّبَة لدى العملاء يعتمدون على برامج حماية تُعزِّز الأَمْن السّيبرانيّ لمَنْع الاختراقات أو تَعَطُّل العمل بالموقع في حال دخول أيّ فيروس.

استعادة البيانات المُسَرَّبَة

إنَّ الأَمْن السّيبرانيّ لا تَقتصر مَهمّته فقط على الحفاظ على البيانات، بل من ضِمن فوائده أنَّه يساعد أيضًا في استرجاع البيانات التي تمَّت سرقتها وتَسريبها في أسرع وقت[1].

1. Sarker, I.H. and Kayes, A.S.M. (2020) Cybersecurity Data Science: An overview from machine learning perspective - journal of big data, SpringerLink. On site: https://link.springer.com/article/10.1186/s40537-020-00318-5

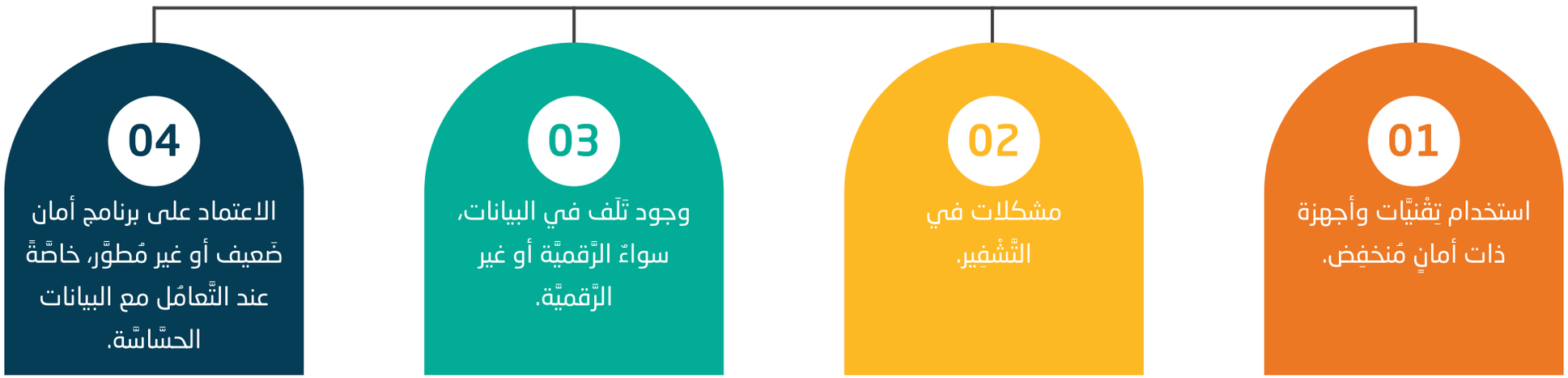
ثالثًا: الفرق بين الأَمْن المَعْلُومَاتيّ والأَمْن السّيبرانيّ

أَمْن المَعْلُومَات

هو الذي يهتمّ بالحفاظ على مدى سِرِّيَّة المعلومات والبيانات التي يقوم مُستخدِم الإنترنت برَبْطها ببعض مواقع التَّواصُل الاجتماعيّ والمِنَصَّات الإلكترونيَّة؛ من أيّ محاولة خرق أو تجسُّس إلكترونيّ، ويتمّ استخدام أَمْن المَعْلُومَات بشكلٍ مُتزايد مع تطوير مواقع الويب وتوسيع أساليبها وأنواعها[1].

المَخَاطِر التي يَتعامل معها أَمْن المَعْلُومَات

من أهمّ المَخَاطِر التي يتعامَل معها أَمْن المَعْلُومَات ما يلي:



1. العتيبي ميعاد (2017م) أساسيات في الأمن السيبراني، مُتَاح على الرَّابط: https://www.docdroid.net/1BTYYas/asasyat-fy-alamn-alsybrany-pdf

ما هي المبادئ الأساسيَّة لأَمْن المَعْلُومَات؟

السِّرِّيَّة:

يهدف هذا المبدأ إلى جعل المعلومات حصريَّة لمن لديه الإذْن بالوصول إليها، وحَجْبها عن أيّ شخص غير مُصرَّح له بالوصول إليها؛ من خلال تشفير المعلومات أو أيّ طُرُق أخرى.

عدم التَّنصُّل والإنكار:

ينصّ هذا المبدأ على أنَّه لا يمكن لأحدٍ أن يُنْكِر تلقّيه لمعلومات أو يدَّعي أنَّها لم تُرسَل إليه؛ حيث نضمن من خلال التَّشْفِير أنَّ المُرسِل قد أرسل المعلومات إلى المُرسَل إليه.

الأصالة:

يهتمّ هذا المبدأ بالتَّأكُّد من أنَّ المُستلِمين همُ الأشخاص الحقيقيُّون الذين نريد إرسال المعلومات إليهم، وليس مُنْتَحِلي الشَّخصيَّة. ويحدث هذا المبدأ نفسه عندما يَتمّ إرسال العُملَات الرَّقميَّة -مثل: البتكوين- من شخصٍ إلى آخر؛ مِن خلال المَحافِظ الرَّقميَّة.

المُساءَلة:

هذا المبدأ يُعْنَى به تتبُّع تصرُّفات الأشخاص الذين وصلوا إلى هذه المعلومات؛ وذلك لضمان معرفتنا بمَن قام بتغيير أو تعديل أيّ جزءٍ من المعلومات، والاحتفاظ بسِجِلّ لهذه الإجراءات للعودة إليه في أيّ وقتٍ.

السَّلامة والنَّزاهة:

يهتمّ بحماية المعلومات من التَّعديل مِن قِبَل الأشخاص غير المُصَرَّح لهم؛ حيث إنَّ هذا المبدأ يُحافظ على دِقَّة وموثوقيَّة البيانات.

إتاحة المعلومات:

يَتعلَّق هذا المبدأ بتَوْفير المعلومات للأشخاص الذين لديهم إذْن بالوصول إليها، في أيّ وقتٍ يحتاجون إليها.

أهم الإجراءات التي يَستخدمها مُتخصِّصو أَمْن المَعْلُومَات

01
كتابة كلمة مرور قويَّة وتغييرها بين الحين والآخر.

02
مُصادَقة ثُنائيَّة أو مُتَعَدِّدَة العوامل؛ مثل رَبْط الموقع الإلكترونيّ برقم الهاتف الجوَّال.

03
إمكانيَّة التَّحكُّم في صلاحيَّة الوصول إلى البيانات.

04
التَّشْفِير.

05
المسؤوليَّة القانونيَّة.

06
الوَعْي الثَّقافيّ.

أَوْجُه التَّشابُه بين الأَمْن السّيبرانيّ وأَمْن المَعْلُومَات

هناك نقاط تَشابُه بين المجالين، وهي:

- يتشابه مجال أَمْن المَعْلُومَات والأَمْن السّيبرانيّ من حيث الاهتمام بأَمْن المَعْلُومَات الإلكترونيَّة أو السّيبرانيَّة.
- يهتمّ الأَمْن السّيبرانيّ بأمن كُلّ ما هو موجود في الفضاء السّيبرانيّ؛ بما في ذلك أَمْن المَعْلُومَات، بينما يهتمّ مجال أَمْن المَعْلُومَات بالحفاظ على المعلومات، حتى لو كانت على الإنترنت.

ما الفَرْق بين الأَمْن السّيبرانيّ وأَمْن المَعْلُومَات؟

- على الرَّغْم من أنّ أَمْن المَعْلُومَات والأَمْن السّيبرانيّ يهتمَّان بحماية المعلومات والحفاظ عليها؛ إلَّا أنَّ الفَرْق بين الأَمْن السّيبرانيّ وأَمْن المَعْلُومَات كبيرٌ من خلال المفهوم والوظيفة.
- يحفظ أَمْن المَعْلُومَات جميع بياناتك عند المُوافَقة على شروط استخدام التَّطبيق الإلكترونيّ، في حين أنَّ الأَمْن السّيبرانيّ يمنع التَّطبيق نفسه من التَّجَسُّس عليك وابتزازك وتَتبُّعك من خلال إظهار اهتماماتك ومُتابعيك على مِنَصَّات التَّطبيق.
- يمكن أن يكون أَمْن المَعْلُومَات عُرْضَة للخرق عند استخدام أنظمة التَّجَسُّس والقَرْصَنَة والفيروسات، في حين أنَّ الأَمْن السّيبرانيّ هو نظام إلكترونيّ يَحْمي الأجهزة من تلقّي أيّ نوع من الفيروسات، ويتمّ إخطار المُسْتَخْدِم بذلك؛ لاتِّخاذ الخطوات المُناسِبة لحماية بياناته من السَّرِقَة.
- يمكن لأَمْن المَعْلُومَات إبلاغك بمحاولة خرق إلكترونيّ لإحدى مِنَصَّاتك أو البيانات التي تَمتلكها، لكنَّ الأَمْن السّيبرانيّ يُمكنه تتبُّع المُتَسَلِّل الإلكترونيّ ومعرفة هُويّته الشَّخصيَّة وجَمْع معلومات عنه، مع ضمان توجيه الاتِّهام الكامل للمُتَسَلِّل قانونًا.

- ينتهي دَوْر أَمْن المَعْلُومَات إذا توقَّف المُسْتَخْدِم عن الإذْن باستخدام معلوماته التي يُوفِّرها في بداية استخدام التَّطبيق مثل تحديد الموقع الجغرافيّ، بينما يُمْكن للأمن السّيبرانيّ تحديد موقع المُسْتَخْدِم ونشاطه وتفاعُله مع البيئة الخارجيَّة؛ من خلال الاتِّصال بأكثر من مِنَصَّة رقميَّة واحدة، وبمساعدة أكثر من برنامج إلكترونيّ يَستخدمه نفس الشَّخص. [1]

1. العتيبي ميعاد (2017م) أساسيَّات في الأَمْن السّيبرانيّ، مرجع سابق.

الفَصْل الثَّاني

المَخَاطِر المُرْتَبِطَة بالأَمْن السّيبرانيّ

- الجرائم الإلكترونيَّة (مَخَاطِر الإنترنت)
- التَّعامُل مع الإساءة عَبْر مواقع التَّواصُل الاجتماعيّ (مَخَاطِر التَّنَمُّر عبر الإنترنت)

0 2

أولًا: الجرائم الإلكترونيَّة (مَخَاطِر الإنترنت)

المقصود بالجريمة الإلكترونيَّة

الجريمة الإلكترونيَّة شَكْلٌ مُتَطَوِّر من أشكال الجريمة العَابِرَة للحدود، التي تَحْدث في مجال الفضاء الإلكترونيّ الذي لا حدود له. ويمكن لمُرتَكِبي الجرائم الإلكترونيَّة وضحاياهم أنْ ينتشروا في مناطق مختلفة، ويمكن أن تمتدّ آثار الجريمة عبر المُجتمَعَات في جميع أنحاء العالَم. وهي نشاطٌ إجراميّ يَستهدف جهاز حاسوب أو شبكة حاسوب أو جهازًا متّصلًا بالشَّبكة، ويحاول استخدامهم بطريقة غير مُصرَّح بها.

تقع معظم الجرائم الإلكترونيَّة على أيدي لُصُوص أو مُخْتَرِقِين يَودّون كَسْب الأموال، وأحيانًا نادرة أخرى يكون الهدف من وراء الجرائم الإلكترونيَّة هو إلحاق الضَّرر بأجهزة الحاسوب لأسباب غير الدَّافع المالي، وقد تكون هذه الأسباب سياسيَّة أو شخصيَّة. ويمكن أن تقع الجرائم الإلكترونيَّة على يَدِ أفراد أو مُنظَّمات؛ وبعض هؤلاء المُجْرِمين الإلكترونيِّين مُنَظَّمُون، ويَستخدمون التّقنيات المُتقدِّمة، وهم ذوو مهارات فنِّيَّة عالية، وبعضهم مُجرَّد مُخترِقِين مُبْتَدِئين[1].

1. Smith, A.D. and Rupp, W.T. (2002), "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers", Information Management & Computer Security, Vol. 10 No. 4, pp. 178-183.

ما هي أنواع الجرائم الإلكترونيَّة؟

- الاحتيال عبر البريد الإلكترونيّ والإنترنت.
- تَزوير الهُوِيَّة (حيث تتمّ سرقة المعلومات الشَّخصيَّة واستخدامها).
- سَرقة البيانات الماليَّة أو بيانات الدَّفْع بالبطاقة.
- سَرقة بيانات الشَّركة وبَيْعها.
- الابتزاز الإلكترونيّ (طلب المال لمَنْع هجوم ضدّ أفراد أو مُؤسَّسَات).
- هجمات برمجيَّات الفِدْيَة (نوع من الابتزاز الإلكترونيّ).
- السَّرِقَة المُشَفَّرة؛ (حيث يقوم المُتَسَلِّلون بتَعْدين العُمَلَات المُشفَّرة باستخدام موارد لا يملكونها).
- التَّجَسُّس الإلكترونيّ (حيث يَتَمَكَّن المُتَسَلِّلون من الوصول إلى بيانات الأفراد والحكومات أو الشَّركات).
- التَّدخُّل في الأنظمة بطريقةٍ تُعرِّض الشَّبكة للخطر.
- انتهاك حقوق النَّشْر.
- المُقامَرَة غير المشروعة.
- بَيْع السِّلع غير المشروعة عبر الإنترنت.

وبهذا نجد أنَّ الجرائم الإلكترونيَّة تشمل أمرَيْن؛ هما:

- نشاط إجراميّ يَسْتهدف أجهزة الحاسوب والهواتف الذَّكيَّة والأجهزة اللَّوحيَّة باستخدام الفيروسات وأنواع أخرى من البرمجيَّات الخبيثة.
- نشاط إجراميّ يَستخدم أجهزة الحاسوب لارتكاب جرائم كالابتزاز.

طريقة عمل مخترقي الأجهزة والبيانات

يُصيب مُرتَكِبُو الجرائم الإلكترونيَّة أجهزة الحواسيب والهواتف الذَّكيَّة والأجهزة اللَّوحيَّة المُستهدَفَة ببرمجيَّات خبيثة لإتلاف الأجهزة أو إيقافها عن العمل، وقد يَستخدمون تلك ببرمجيَّات الخبيثة في حَذْف البيانات أو سرقتها.

ويمكن لمخترقي الأجهزة والبيانات أيضًا بواسطة البرمجيَّات الخبيثة مَنْع المُسْتَخْدِمين من استخدام موقع إلكترونيّ أو شبكة الإنترنت، أو مَنْع مُؤسَّسَة تُقدِّم خدمةً ما من الوصول إلى عملائها، وهذا الأسلوب معروف باسم هجوم الحِرْمان من الخِدْمَات؛ كما تشمل الجريمة الإلكترونيَّة تثبيّت البرمجيَّات الضَّارَّة على الحواسيب والأجهزة الذَّكيَّة، ونشر هذه البرمجيَّات على الشَّبكات.

وغالبًا ما يَفْعَل مُرتكبو الجرائم الإلكترونيَّة الأمرين في الوقت نفسه؛ فهُم يَسْتَهْدِفُون أجهزة الحاسوب التي تحتوي على فيروسات أولًا، ثمَّ يستخدمونها لنَشْر البرمجيَّات الخبيثة على أجهزة أخرى أو عبر الشَّبكة[1].

1. Person, Tim, P. and Jordan, T. (2017) A sociology of hackers: 10: Cyberspace crime: Tim Jordan, Paul Tayl, Taylor & Francis. On site: https://cutt.us/NwnyZ

ما الأخطاء الشَّائعة التي يقع فيها مستخدمو الإنترنت؟

يقع مُسْتَخْدِمُو الإنترنت في عددٍ منَ الأخطاء، والتي من الممكن أن يَستثمرها القراصنة الرَّقميُّون لتنفيذ هجماتهم، وفيما يلي تبيان لأهمّ هذه الأخطاء:

1. **كلمات مرور مُتشابِهَة:** من الضَّروريّ تجنُّب وَضْع كلمة مرور واحدة لجميع حساباتك الشَّخصيَّة وبريدك الإلكترونيّ، فعند خرق حساب واحد تتسبَّب في سرقة جميع حساباتك وخرقها بشكلٍ كاملٍ، وتعريض بياناتك للخطر.
2. **إعدادات الخصوصيَّة:** من أخطر الأخطاء التي يَتمّ ارتكابها على مواقع التَّواصُل الاجتماعيّ هو تجاهُل إعدادات الخصوصيَّة، وعدم مُتابَعَة أحدث التَّغييرات التي تُجريها المواقع المختلفة لحماية المُسْتَخْدِمين.
3. **عدم امتلاك نظام آمِن:** يتجاهل الكثير من المُسْتَخْدِمين تحديث أنظمة أجهزتهم الذَّكيَّة؛ سواءٌ الأجهزة اللوحية أو الهواتف، ممَّا يُعرِّضهم لعشرات الثَّغرات التي قد يَستغلّها مخترقو الأجهزة والبيانات لسرقة البيانات واختراق الأجهزة.
4. **الرَّوَابِط:** رغم تحذيرات الخبراء من عدم الضَّغْط على أيّ رابط غير معروف؛ إلَّا أنَّ هناك العشرات من المُسْتَخْدِمين الذين يرتكبون هذا الخطأ؛ ممَّا يتسبَّب في خرق حساباتهم.
5. **طلبات الصَّداقة:** يُعدّ قَبُول طلبات الصَّداقة من أشخاص لا تَعرفهم ولا تربطك بهم أيّ علاقة أمرًا خطيرًا؛ حيث تعطيهم الحقّ والصلاحيَّة لاختراق خصوصيتك ومعرفة معلوماتك الشَّخصيَّة.
6. **مُشارَكة المعلومات الشَّخصيَّة:** من الأخطاء التي لا يُدركها المستخدمون مشاركة الكثير من التَّفاصيل عن حياتهم الشَّخصيَّة، وطبيعة عملهم ومنزلهم.

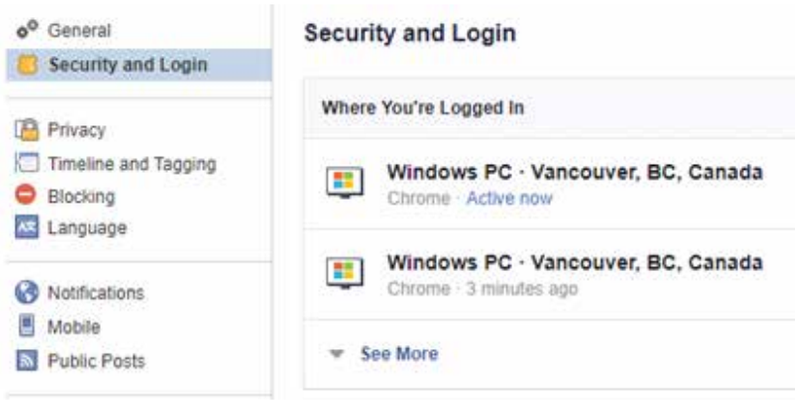
كيف يَتمّ التَّعامُل مع خرق الحساب الشَّخصيّ على مواقع التَّواصُل الاجتماعيّ؟

إذا كنتَ تَشُكّ في أنَّ كلمة مرور حسابك على مواقع التَّواصُل الاجتماعيّ الخاصَّة بك قد سُرِّبَتْ، أو أنَّ حسابك مُخْتَرَق؛ فعليك التَّصرُّف بسرعةٍ؛ حيث يمكن للمُتَسَلِّلين مَنْعُك من الدُّخُول إلى حسابك وإزعاج أصدقائك وعائلتك؛ لذا يجب تأمين حسابك بسرعةٍ أو استعادته قبل فَوَات الأوان.

كيف تعرف أنَّ حسابك مُخْتَرَق؟

إذا تَمَكَّن أحد المُتَسَلِّلين من الدُّخُول إلى حسابك، فسوف يَتْرُك أثرًا، ويمكن معرفة ذلك من خلال:

- انْقُر على السَّهم في الجزء العُلْوِيّ الأيمن.
- من القائمة، اخْتَرْ (الإعدادات) Settings.
- انْتَقِل إلى (الأمان وتسجيل الدُّخُول) Security and Login.
- في الجزء العُلْوِيّ، سترى قائمةً بالأجهزة التي قُمتَ من خلالها بتسجيل الدُّخُول إلى حسابك خلال الفترة الأخيرة، ومتى كانت نَشِطَة.
- انْقُر على (عَرْض المزيد) See More، لفَتْح تلك القائمة، ومُراجَعة الجلسات القديمة.



إذا لاحظتَ أيّ نشاط مُريب في تسجيلات الدُّخُول الخاصَّة بك، فعليكَ القيام بالآتي:

تغيير كلمة المرور:

- في حال لم يُغيِّر المُخْتَرِق كلمة المرور، فأنتَ محظوظٌ، فهذا هو الوقت المُناسِب لتحديث كلمة مُرُورك قبل تسجيل الخروج من الجلسات غير المعروفة.
- اضْغَطْ على قائمة (الإعدادات).
- اضْغَطْ على خيار (الأمان وتسجيل الدُّخُول).
- قُمْ بالتَّمرير لأسفل للوصول إلى خيار (تسجيل الدُّخُول) Login.
- انْقُر على (تغيير كلمة المرور) Change password.
- أَدْخِل كلمة المرور الحاليَّة، وقمْ باختيار كلمة مرور جديدة قويَّة، أو يمكنك استخدام تطبيق مدير كلمات مرور (مثل: Last Pass)، ثم اضْغط على خيار (حِفْظ التَّغييرات) Save Changes.

الإبلاغ عن الاختراق:

إذا وجدتَ أنَّ حسابك لم يُختَرق، ولكنَّه بدأ بإرسال رسائل غير مَرْغُوب فيها إلى أصدقائك، فيجب عليك إبلاغ إدارة موقع التَّواصُل الاجتماعيّ عن ذلك، كإدارة Facebook، من خلال استخدام رابط: Facebook.com/hacked/.

إزالة التَّطبيقات المشكوك فيها:

أحيانًا، يكون خرق حسابك من خلال التَّطبيقات التي مَنَحْتَها حقّ الوصول إليه وإعطائها بعض الأذونات، ولإزالة مثل هذه التَّطبيقات اتَّبِع الآتي:

- انْتَقِلْ إلى (الإعدادات) في حسابك.
- اضْغَطْ على خيار (التَّطبيقات ومواقع الويب) Apps and Websites.
- من القائمة، اضْغَطْ على خيار (إظهار الكُلّ) Show All، لرؤية (التَّطبيقات ومواقع الويب النَّشِطَة) Active Apps and Websites.
- حَدِّد التَّطبيق أو مواقع الويب التي تَشتبه فيها، ثم اضْغَطْ على زِرّ (إزالة) Remove، في الجزء العُلْوِيّ الأيسر.
- أكِّد ما إذا كنت ترغب أيضًا في (حَذْف جميع المُشارَكات والصُّور ومَقاطع الفيديو في فيسبوك) من هذه المصادر.

التَّحكُّم في الضَّرر:

بعد القيام بكلّ ما في وُسْعك لاستعادة السَّيطرة على حسابك في Facebook، ومَنْع المزيد من الضَّرر، أَخْبِرْ أصدقاءَك وعائلتك بما حدَث؛ حيث تُعدّ هذه الخطوة احترازيَّة في حالة إساءَة المُخْتَرِق لاستخدام حِسَابك.

وإذا لم تتمكَّن حاليًّا من الوصول إلى حسابك؛ فاتَّصِل بأصدقائك في Facebook، من خلال مواقع التَّواصُل الاجتماعيّ الأخرى، أو عَبْر البريد الإلكترونيّ، أو اطْلُب من صديق مُشْتَرَك إبلاغهم عَبْر Facebook.

كيف أحْمِي نَفْسِي من الجرائم الإلكترونيَّة؟

فيما يلي بعض النَّصائح البسيطة لحماية أجهزتك الإلكترونيَّة وبياناتك الشَّخصيَّة من الجرائم الإلكترونيَّة:

إبقاء البرنامج ونظام التَّشْغيل مُحدَّثَيْن

يضمن إبقاء البرنامج ونظام التَّشْغيل في جهازك، كالحاسوب أو الهاتف، مُحدَّثَيْن؛ استفادتك من أحْدَث تَصْحيحات الأمْن لحماية أجهزتك الإلكترونيَّة.

استخدام برنامج مُكَافَحَة الفيروسات وتحديثه باستمرار

يُشَكِّل استخدام برنامج لمُكَافَحَة الفيروسات طريقة ذكيَّة لحماية النِّظام من الهجمات الخبيثة، فهو يُتيح لك إمكانيَّة فَحْص التَّهْديدات واكتشافها وإزالتها قبل أن تُصْبِح مشكلة، وبالتَّالي حماية جهاز الحاسوب الخاصّ بك وبياناتك من الجرائم الإلكترونيَّة.

استخدام كلمات مرور قويَّة

تأكَّد من استخدام كلمات مرور قويَّة لا يمكن للأشخاص مَعْرفتها، ولا تَقُم بتسجيلها في أيّ مكان، ويمكن كذلك استخدام "تطبيق مدير كلمات مرور" حَسَن السُّمْعَة؛ لإنشاء كلمات مرور قويَّة بشكلٍ عشوائيّ؛ لتسهيل الأمر عليك كما يجب تغيير كلمات المرور بين الحين والآخر.

تَجاهل المُرْفَقات في رسائل البريد الإلكترونيّ العشوائيَّة

تُشكِّل مُرفَقات البريد الإلكترونيّ في رسائل البريد الإلكترونيّ العشوائيَّة طريقة تقليديَّة لإصابة الأجهزة الإلكترونيَّة ببرمجيَّات ضارَّة، وغيرها من أشكال الجرائم الإلكترونيَّة. لذا لا تفتح أبدًا مرفقًا من مُرْسِل لا تَعرفه.

عدم فَتْح الرَّوَابِط

توجد طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونيَّة، وهي فَتْح الرَّوَابِط الموجودة في رسائل البريد الإلكترونيّ العشوائيَّة أو الرَّسَائل الأخرى أو المواقع الإلكترونيَّة غير المألوفة، فلا تَقُم بذلك للحفاظ على أَمْنِكَ على الإنترنت.

الامتناع عن تقديم المعلومات الشَّخصيَّة إلا إذا كنت آمِنًا

لا تُقدِّم أبدًا بيانات شخصيَّة عبر الهاتف أو عبر البريد الإلكترونيّ إلى أيّ جهةٍ؛ ما لم تكن مُتَأكِّدًا تمامًا من أمان الخطّ أو البريد الإلكترونيّ. وتأكَّد من أنَّك تتحدَّث إلى الشَّخص الذي تعتقد أنَّك تتحدَّث معه.

الاتِّصال بالشَّركات مباشرةً بشأن الطَّلبات المريبة

إذا اتَّصَلَتْ بك شركةٌ، وطلبتْ منك معلوماتٍ شخصيَّةً أو بياناتٍ؛ قُمْ بإنْهَاء المُكالَمة بدون إعطائهم أيّ معلومة، ثم أَعِد الاتِّصال بهم مرَّة أخرى باستخدام الرَّقم الموجود على الموقع الإلكترونيّ الرَّسميّ الخاصّ بهم؛ للتَّأكُّد من أنَّك تتحدَّث إليهم وليس مع مُجْرمي الإنترنت. والأفضل كذلك استخدام رقم هاتف مختلف؛ لأنَّ مُجْرمي الإنترنت يمكنهم إبقاء الخطّ مفتوحًا.

التَّنبُّه لعناوين مواقع URL التي تزورها

رَاقِب عناوين مواقع URL التي تفتحها. هل تبدو مشروعة؟ تجنَّب الضَّغْط على الرَّوَابِط التي تحتوي على عناوين URL غير مألوفة، أو التي تبدو كرسالة غير مَرغُوب فيها. إذا كان مُنْتَج أمْن الإنترنت لديك يشمل وظائف ضمان أمْن المعاملات عَبْر الإنترنت؛ فتأكَّد من تمكينها قبل تنفيذ المعاملات الماليَّة عبر الإنترنت.

ثانيًا: التَّعامُل مع الإساءة عبر مواقع التَّواصُل الاجتماعيّ (مَخَاطِر التَّنَمُّر عبر الإنترنت)

ما هو التَّنَمُّر عبر الإنترنت؟

التَّنَمُّر عبر الإنترنت هو التَّنَمُّر باستخدام التّقنيات الرَّقميَّة. ويمكن أن يحدث عبر وسائل التَّواصُل الاجتماعيّ، ومِنَصَّات التَّراسُل، ومِنَصَّات الألعاب الإلكترونيَّة، والهواتف الذَّكيَّة، وهو سلوك مُتكرّر يهدف إلى تخويف الأشخاص المُستهدَفين أو إغضابهم أو التَّشْهير بهم.

ومن بين الأمثلة على هذا النّوع من التَّنَمُّر:

01
نَشْر الأكاذيب أو نَشْر صُوَر مُحْرِجَة لشَخْص ما على وسائل التَّواصُل الاجتماعيّ.

02
إرسال رسائل أو صُوَر أو مقاطع فيديو مُؤذِيَة أو مُسيئَة أو تهديدات عبر مِنَصَّات التَّراسل.

03
سرقة هُوِيَّة أحدٍ ما، وتوجيه رسائل مسيئة للآخرين باسمه، أو من خلال حسابات وَهْميَّة.

كيف يمكننا تمييز الفَرْق بين المزاح وبين التَّنَمُّر عبر الإنترنت؟

من عادة الأصدقاء أن يمزحوا مع بعضهم، ولكن أحيانًا من الصَّعب أن نُحدِّد ما إذا كان شخصٌ ما يمزح أم يسعى إلى التَّسبُّب في الأذَى، خصوصًا عبر الإنترنت، وينتهي الأمر بقول: "كنت أمزح فقط"، أو "لا تأخذ الأمور بجدّيَّة زائدة". وفي حال أحْزَنَتْكَ الكلمات أو كنتَ تعتقد أنَّ الشَّخص الآخر يَضْحَك عليكَ بدلًا من أن يَضْحَك معك؛ فحينها تكون المزحة قد تجاوزت حدودها. وإذا استمرَّ الأمر بعد أن تطلب من الشَّخص التَّوقُّف، أو شعرتَ بالانزعاج بهذا الشَّأن؛ فحينها قد يكون الأمر تَنمُّرًا عبر الإنترنت.

كيف يمكن للتَّنَمُّر عبر الإنترنت أن يُؤثِّر في صِحّتي العقليَّة؟

تتنوَّع تأثيرات التَّنَمُّر الرَّقميّ في الصِّحَّة العقليَّة بناءً على الوسط الذي تحدث من خلاله، فالتَّنَمُّر عبر الرَّسَائل النَّصِّيَّة الهاتفيَّة أو عبر صُوَر أو مقاطع فيديو عبر مِنَصَّات التَّواصُل الاجتماعيّ مُؤْذٍ جدًّا للمُراهِقِين لشُعُورهم بالخِزْي، أو التَّوتُّر، أو القَلَق أو عدم الثِّقة بالنَّفس إزَاءَ ما يقوله النَّاس عنهم أو ما يُفكِّرون به حِيَالَهم.

وقد يُؤدِّي هذا إلى الابتعاد عن الأصدقاء والأسرة، وإلى نُشوء أفكار سلبيَّة والشُّعور بالوحدة، أو أنَّ الْعِبْء يَفُوق قدرتك على التَّحمُّل، أو يُصيبك بالصّداع المُتَكَرِّر، أو الغَثَيَان، أو الألم.

ومن التَّأثيرات الشَّائعة الأخرى للتَّنَمُّر عبر الإنترنت: التَّغيُّب عن المدرسة، كما قد يُؤثِّر في صِحَّة اليافعين.

كيفيَّة التَّعامُل مع المُتنمِّرين عبر الإنترنت

- الخُطوة الأُولَى هي التَّحدُّث إلى شخصٍ تَثِق به مِن قَبيل صديق أو فرد من الأسرة أو مُرشِد اجتماعيّ في المدرسة، أو شَخْص بالِغ آخر تَثِق به.
- إذا كان التَّنَمُّر يحدث عبر وسائل التَّواصُل الاجتماعيّ، فينبغي أن تُفكِّر في حَجْب الشَّخص الذي يمارس التَّنَمُّر، والإبلاغ عن سُلُوكه إلى موقع التَّواصُل الاجتماعيّ المعنيّ، فشركات مواقع التَّواصُل الاجتماعيّ مُلزَمة بالمُحافَظة على سلامة المُسْتَخْدِمين.
- من المفيد أن تجمع أدِلَّة مثل رسائل نصيَّة أو صورة تتضمَّن المواد المُسيئة المنشورة عبر مواقع التَّواصُل الاجتماعيّ ضِدَّك والإبلاغ عنه.
- فَكِّر مرَّتين قبل أن تنشر أو تشارك أيّ شيءٍ على شبكة الإنترنت؛ فقد يَظَلُّ موجودًا على الإنترنت إلى الأبد، ويمكن أن يُستخدَم لإيذائك لاحقًا.
- لا تُعطِ أيّ تفاصيل شخصيَّة مِن قَبيل عُنوانك، أو رقم هاتفك، أو اسم مدرستك.
- تعرَّف على إعدادات الخصوصيَّة على تطبيقات التَّواصُل الاجتماعيّ المُفضَّلة لديك.

1. فرعون، سامر عبدالكريم. حِمايَة حقوق المُؤَلِّفين الفِكْرِيَّة على الإنترنت. - مِجلَّة حماية المِلْكِيَّة الفِكْرِيَّة. - ع 55، الربع الأول (1998م).

الإجراءات التي يمكنك اتِّخاذها للوقاية من التَّنَمُّر عبر الإنترنت

يمكنك أن تُقرِّر مَن يرى المنشورات على حسابك، أو إرسال رسائل أو تعليقات مُباشِرَة حول الموادّ التي تَنْشرها، وذلك بتعديل إعدادات الخصوصيَّة في حسابك.

بوُسْعك الإبلاغ عن التَّعليقات والرَّسَائل والصُّور المُؤذِيَة، وأن تَطْلب إزالتها.

إضافةً إلى إلغاء الصَّداقة؛ يمكنك أن تَحْجب أفرادًا مُعَيَّنين لمَنْعهم من رؤية حسابك أو الاتِّصال بك.

بوُسْعك أيضًا أن تختار توجيه تعليقات أشخاص مُحدَّدين؛ كي تظهر لهم فقط دون أن تحجبهم تمامًا.

يمكنك إزالة موادّ من معلوماتك أو إخفاؤها عن أشخاص مُعيّنين.

الفَصْل الثَّالث

كيف أحمي نفسي من التَّهْديدات الرَّقميَّة؟

- استخدام كلمة المرور لحماية البيانات
- حماية البريد الإلكترونيّ
- ماذا أفعل عند تَعرُّضي للتَّهديدات الرَّقميَّة؟

0 3

أولًا: استخدام كلمة المرور لحماية البيانات

من خلال إنشاء كلمة مرور قويَّة، يمكن لمُستخدِم الإنترنت الاستفادة بالآتي:

كيف تكتب كلمة مرور قويَّة؟

ينبغي أن تَتَأَلَّف كلمة المرور من أيّ مجموعة من الأحرف والأرقام والرُّموز (أحرف ASCII العاديَّة فقط)، ولا يمكن استخدام أحرف مُشكّلة.

ولا ينبغي استخدام كلمة مرور:

للحصول على كلمة مرور قويَّة يُفضَّل اتّباع الآتي

01
تُعتبر كلمة المرور قويَّة عندما يَسْهُل عليك أن تَتَذَكَّرها، ويكاد يكون مُستحيلًا على أيّ شخص آخر تَخْمينها.

02
اسْتَخْدِم كلمة مرور مختلفة لكلّ حساب من حساباتك المهمَّة، مثل بريدك الإلكترونيّ، وصفحاتك عبر الإنترنت.

03
من الخطر تكرار استخدام نفس كلمات المرور في حساباتك المُهمَّة؛ فإذا حصل أحدهم على كلمة مرور أحد حساباتك؛ يتمكَّن من الوصول إلى بريدك الإلكترونيّ وباقي حساباتك.

04
استخدام كلمة مرور طويلة يسهل تذكّرها، إذ تَتَمَيَّز كلمات المرور الطويلة بقُوّتها، لذا يجب ألّا تكون كلمة المرور أقلّ من 12 حرفًا.

وفيما يلي نصائح تُساعدك على كتابة كلمات مرور طويلة يسهل عليك تذكُّرها؛ حيث يُمكنك استخدام ما يلي:

- كلمات من أغنية أو قصيدة.
- مَقُولة مُميَّزة من فيلم أو خِطاب.
- فقرة من كِتَاب.
- سلسلة كلمات ذات مغزًى بالنِّسبة إليك.
- اختصار: تكوين كلمة مرور من الحَرْف الأوَّل من كُلّ كلمة في جُمْلة معيَّنة.

مع تجنُّب اختيار كلمات مرور سهلة يمكن تَوقُّعها أو تَخْمينها، مثل:

- أشخاص يعرفونك.
- معلومات يمكن مَعْرفتها من خلال ملفّك الشَّخصيّ على وسائل التَّواصُل الاجتماعيّ.

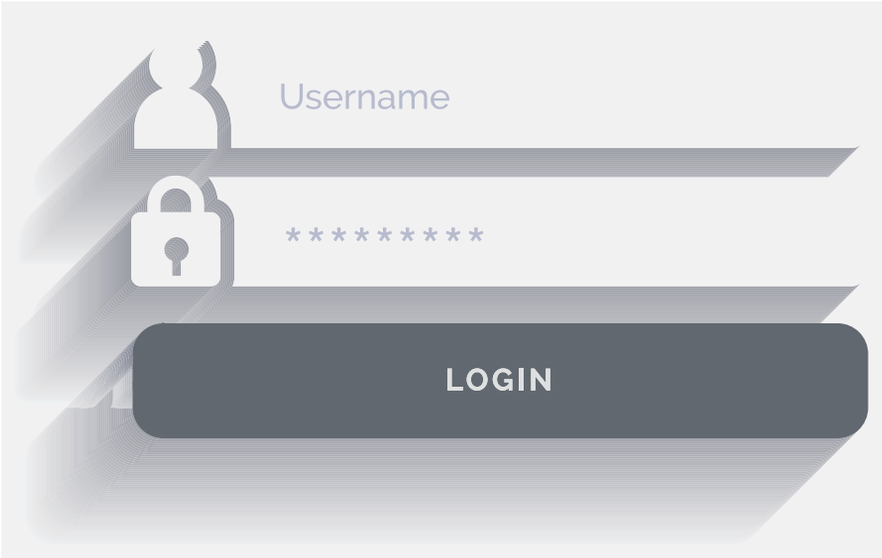
- تجنَّب استخدام معلومات قد يكون الآخرون على عِلْمٍ مُسْبَق بها، أو يمكنهم الوصول إليها بسهولةٍ، مثل:

  - لَقَبك أو الأَحْرُف الأُولَى من اسمك.
  - اسم حيوانك الأليف.
  - أعياد الميلاد أو السَّنوات المُهمَّة لك.
  - اسم الشَّارع الذي تسكن فيه.
  - أرقام من عنوانك.
  - رقم هاتفك.

- **تجنَّب استخدام الكلمات والعبارات والأنماط البسيطة التي يَسْهل تَخْمينها. مثل:**

  - الكلمات والعبارات الواضحة، مثل "password".
  - الأَحْرُف أو الأرقام المُتَتابِعَة مثل "abcd" أو "1234".
  - أنماط لَوْحة المفاتيح، مثل "qwerty" أو "qazwsx".

- **إذا أردتَ تدوين كلمة مرورك، لا تحفظها على أجهزتك الإلكترونية أو مَكْتبك، تأكَّد من حِفْظ أيّ كلمات مرور مكتوبة في مكان سِرِّي أو مُؤمَّن.**



ثانيًا: حماية البريد الإلكترونيّ

حماية البريد الإلكترونيّ من الاختراق والقَرْصَنَة؛ تعني حمايتك من عمليَّات الاحتيال والنَّصب والبرمجيَّات الضَّارَّة، والتي تتمّ عبر تتبُّع رسائل البريد الإلكترونيّ والرَّوَابِط التي أُرسلت إليك من شخصٍ ما، فيتمّ الدُّخُول إلى حسابك من تلك التَّفاصيل والرَّوَابِط المُرسَلة إليك.

ومن أهمّ الخطوات التي يجب عليك اتّباعها من أجل حماية حساب البريد الإلكترونيّ الخاصّ بك من مخترقي الأجهزة والبيانات ومُجْرِمي الإنترنت:

اختيار كلمة مرور قويَّة

حسابات البريد الإلكترونيّ التي تحتوي على كلمات المرور الضَّعيفة، هي الأكثر عُرْضَة للاختراق، وغالبًا ما يَسْهُل الوصول إليها، ويجب أن تَختار كلمات بعيدة عن التَّخمين، وتكون طويلة، والمَزْج فيها بين الأحرف الكبيرة والصَّغيرة والأرقام والرُّمُوز.

تفعيل مَيْزَة "التَّحقُّق بخطوتين"

هي أحد أهمّ الأمور التي يجب عليك تفعيلها في حساب البريد الإلكترونيّ (Email) الخاصّ بك، من أجل حمايته وتجنُّب تعرُّضه للاختراق؛ حيث إنَّ تفعيل هذه الخاصيَّة يجعل المُسْتَخْدِم مُطالَبًا بإدخال أكثر من وسيلة تَحقُّق للسَّمَاح له بالدُّخول إلى حسابه.

حيث يَجِب عليه إدخال كلمة المرور، بالإضافة إلى وسيلة أمان ثانية، تتمثَّل بإرسال رسالة نصيَّة تحتوي على رمز أمان لتسجيل الدُّخُول، يَتمّ إرسالها إلى رقم هاتف المُستخدِم، ويُوفِّر معظم مُزوّدي خِدْمَات البريد الإلكترونيّ هذه الخاصيَّة عبر الحسابات الخاصَّة بجميع المُسْتَخْدِمين.

تغيير كلمات المرور بشكلٍ دَوْريّ

يُعدّ تغيير كلمات المرور بشكلٍ دَوْريّ واحدًا من أهمّ الأسباب التي قد تَمنع الآخرين من الوصول أو استخدام حسابك، فإنْ حدَث أنَّ شخصًا ما قد حصَل على كلمة المرور الخاصَّة بحسابكَ؛ فإنَّها لا تكون كلمة المرور الحاليَّة، بل هي كلمة مرور سَابقة.

استخدام كلمات مُرور مختلفة

إنَّ استخدام كلمة مرور واحدة على كافَّة المواقع المُتعلِّقة بنفس حساب البريد الإلكترونيّ، يُعدّ خطيرًا على جميع حساباتك، وبالتَّالي إذا تمَّ اختراق كلمة المرور لموقع إلكترونيّ واحد، فإنَّه يمكن أن يَتمّ استخدامها للدُّخُول إلى جميع حساباتك على المواقع أخرى.

تحديث البرامج الموجودة على الجهاز

يُعدّ تحديث البرامج الموجودة على الجهاز الخاصّ بك، أمرًا في غاية الأهميَّة للحفاظ على حسابك وحمايته من التَّعرُّض للاختراق؛ حيث يجب عليك دائمًا الاستمرار في تحديث تطبيق البريد الإلكترونيّ، ومُتصفِّح الإنترنت الذي تَستخدمه عادةً للوصول إلى حِساباتك، بالإضافة إلى تحديث أيّ تطبيقات أخرى على جهازك.

علاوةً على ذلك، يجب أن تتأكَّد دائمًا من تحديث نظام التَّشْغيل الذي يعمل به الجهاز، في حال صدور أيّ تحديثات لنظامه، سواءٌ كان ذلك نظام Windows أو Mac على الحاسوب، أو Android أو iOS على الهواتف الذكيَّة؛ حيث عادةً ما تشتمل هذه التَّحديثات على تحديثات أمنيَّة لإغلاق الثَّغرَات وإصلاح الأخطاء الموجودة في الأنظمة والتَّطبيقات.

حَظْر مصدر البريد العشوائيّ ذي المحتوى المجهول

يمكن للكثير من القراصنة المُخْترِقين؛ استخدام الرَّسَائل الإلكترونيَّة والرَّسَائل النَّصيَّة وصفحات الويب، في خرق الحسابات وانتحال هُويَّة المُؤسَّسَات والأفراد، والدُّخُول إلى حِساباتهم الشَّخصيَّة؛ وذلك عَبْر إرسال رسائل وَهْميَّة تحتوي على رَوَابط أو ملفَّات تَتَضمَّن بداخلها بعض الفيروسات والبرمجيَّات الخبيثة، وبمُجَرَّد فَتْحها أو النَّقْر عليها، يَتمّ الوصول إلى حساباتك وسرقة بياناتك.

لتفادي هذا النَّوع من الاختراقات؛ يجب عليك تجنُّب فَتْح رسائل البريد العشوائيّ، والرَّسَائل ذات المحتوى المجهول، وعدم فَتْح الرَّوَابِط والمِلَفَّات غير الموثوقة وصفحات الويب المريبة.

تتبُّع رسائل البريد الإلكترونيّ المجهول

يمكنك تتبُّع رسائل البريد الإلكترونيّ؛ إن لم تكن مُتأكِّدًا من مصدر الرِّسَالة والهدف الأساسيّ منها؛ حيث يُتِيح لك معظم مُقدِّمي خِدْمَات البريد الإلكترونيّ، إمكانيَّة تتبُّع رسائل البريد الإلكترونيّ، ومعرفة مَصْدرها، وهي إحدى الخطوات المُهمَّة، التي يجب عليك اتِّخاذها في التَّعامُل مع رسائل البريد الإلكترونيّ.

وللقيام بذلك في الـ Gmail اتَّبع الخطوات التَّالية:

1. افْتَح حساب Gmail الخاصّ بك، باستخدام أيّ مُتصفِّح.
2. افْتَح رسالة البريد الإلكترونيّ التي تريد تتبُّعها.
3. انقر فوق رمز المزيد (⋮) بجوار كلمة "رد"، الموجود في الزاوية العُلْويَّة من الرِّسَالة.
4. حَدِّد "عَرْض النُّسخة الأصليَّة" من القائمة.
5. سيتمّ فَتْح نافذة جديدة تحتوي على معلومات الرِّسَالة الأصليَّة؛ بما في ذلك: نتائج المُصادَقة، وعنوان "أي بي" (IP) الخاصّ بالمرسل، وتاريخ الإنشاء، ورقم تعريف الرِّسَالة.

ولتَتَبُّع رسائل البريد الإلكترونيّ في خِدْمَات البريد الأخرى من خلال التَّالي:

01 في Outlook:
انْقُر على "ملفّ"، ثمّ على "الخصائص".

02 في Hotmail:
انْقُر بزرّ الماوس الأيمن على الرِّسَالة الإلكترونيَّة، ثم حدِّد "عَرْض مصدر الرِّسَالة".

03 في Apple Mail:
انْقُر على "عَرْض"، ثمَّ "الرِّسَالة"، وحَدِّد "جميع العناوين".

04 في Yahoo:
انْقُر على "المزيد"، ثمَّ حدِّد "عرض الرِّسَالة الأصليَّة".

مع العلم أنَّ جميع الخطوات السَّابقة ستُؤدِّي إلى إظهار العناوين، إمَّا في نافذة جديدة أو في مربع عنوان الإنترنت؛ حيث يمكنك الاطِّلاع على مصدر رسائل البريد الإلكترونيّ قَبْل فَتْحها، وإذا كانت لديك أيّ شكوك حول هذه الرَّسَائل، فيمكنك إمَّا إلغاء الاشتراك في خدمة تلقّي الرَّسَائل من المصدر، أو حَظْر مصدر البريد المجهول.

ثالثًا: ماذا أفعل عند تَعرُّضي للتَّهديدات الرَّقميَّة؟

التَّعامُل مع حالات الابتزاز الإلكترونيّ

في حال تَعرُّضك للابتزاز الإلكترونيّ... عليك بالآتي:

- لا تُحاوِل الرَّدّ على الشَّخص المُبتَزّ أو إقناعه بعدم نَشْر معلوماتك وصُوَرك الشَّخصيَّة؛ فهذا يُعْطِي انطباعًا بأنَّك ضَعْيف أو مُستجِيب لمَطالبهم، ما يَدْفعهم إلى زيادتها أو التَّحقُّق من صِحّتها.
- قمْ بتخزين المحتوى الذي تمَّ ابتزازك به، مع عدم حَذْف رسائل التَّهْديد؛ فهي دليلٌ يمكن استخدامه لإدانة المُجْرِمين.
- وَقْف متابَعَة المُبتزّ لحساباتك على مواقع التَّواصُل الاجتماعيّ، وتغيير كلمات المرور الخاصَّة بك على الفَوْر، فيُفضَّل استخدام كلمات مرور مختلفة تتضمَّن أرقامًا وحروفًا ورموزًا لحساباتك المُتنوّعة.
- أخْبِر شخصًا موثوقًا بما حدَث لك مثل الأب أو الأم أو مُشْرفك في المدرسة؛ لتزويدك بالدَّعْم النَّفسيّ، كما يُفضَّل طَلَب الدَّعْم النَّفسيّ من مُتخصِّصين؛ كي لا يُؤثِّر الابتزاز في صِحّتك العقليَّة والنَّفْسيَّة.
- تواصل مع إدارة مكافحة الجرائم الإلكترونيَّة بوزارة الدَّاخليَّة.

حماية البيانات الشَّخصيَّة من السَّرِقَة

الأمثلة

الأمْثِلَة المَذْكُورَة أدناه قد تتضمَّن معلومات تَفُوق قُدْرَة الطَلبة على فَهْمها، لذلك يُرْجَى من المُدَرِّب تَقْديمها بصُورَة مُبسَّطة، والهدف منها تقديم حقائق للطَّلبة حول الآثار التي تسببها الجرائم الإلكترونيَّة، وتمَّ التَّوسُّع في الأمثلة وإضافَة بعض المراجع، بحيث يَتمكَّن المُدَرِّب من التَّوسُّع بالفكرة والإحاطة بها، حتى يَتَسَنَّى له تقديم معلومات دقيقة وبسيطة في ذات الوقت.

المثال الأوّل: فيروس «Melissa»[1]

في عام 1999م، ظهر فيروس أُطْلِقَ عليه «Melissa»، وكان يُعدّ الأشهر بين الفيروسات التي تُصيب الأجهزة الإلكترونيَّة في تلك الفترة، بعد تسبُّبه في غَلْق نُظم البريد الإلكترونيّ، والتي تكدَّست برسائل البريد الإلكترونيّ المُصابَة المنبعثة من الفيروس، ما تسبَّب في خسائر فادحة.

وكان هذا الفيروس يُرسَل داخل ملفّ يدعى "List.DOC" يحتوي على كلمات مرور لـ 80 موقعًا خبيثًا، وتمَّ إرسال النموذج الأصليّ للفيروس عبر البريد الإلكترونيّ للعديد من الأشخاص.

وعمل الفيروس على إصابة العديد من الأجهزة عَقِب فَتْحه مُباشَرة عبر نَسْخ نفسه عبر البريد الإلكترونيّ؛ حيث يجمع أوَّل 50 اسمًا من قائمة العناوين، ويرسل رسائل إلكترونيَّة لهذه العناوين البريديَّة، كما عمل على إخفاء ملفَّات مُهمَّة.

وألقت الشُّرطة الأمريكيَّة القَبْض على مُبْتَكِر الفيروس الذي أطلق على نفسه اسم «كويجبو»، وحُكِمَ عليه بالسجن لمدَّة 40 عامًا، ودَفع غرامة ماليَّة بقيمة نصف مليون دولار أمريكيّ.

1. . Melissa Virus, FBI, on site: https://cutt.us/m1J9f

المثال الثَّاني: دودة مورس[1]

في عام 1988م، تمكَّن روبرت موريس البالغ من العمر (23 عامًا)، من إطلاق فيروس «دودة مورس» على شبكة الإنترنت، وهي أوَّل هجمة إلكترونيَّة ضَخْمة تمَّت على الشَّبكة وتَسبَّبت بإصابة 6 آلاف جهاز حاسوب، يرتبط بها أكثر من 60,000 نظام إلكترونيّ للمُؤسَّسات والدَّوائر الحكوميَّة.

وقُدِّر حَجْم الخسائر النَّاتجة عن «دودة مورس» بما يقرب من 100 مليون دولار أمريكيّ، حتى تمكَّنت الحكومة الأمريكيَّة من إعادة تشغيل الأنظمة من جديد.

وحُكم على «موريس» بالسجن لمدة 3 أعوام ودَفع غرامة ماليَّة بقيمة عشرة آلاف دولار أمريكيّ ووضعه تحت المُراقبة بعد خروجه من السّجن.

المثال الثَّالث: برنامج فِدْيَة «Reveton»[2]

في عام 2012م، بدأ ينتشر برنامج فِدْيَة اسمه «Reveton»، والذي يعمل على إظهار تحذير يُنسَب إلى وكالة تطبيق القانون، يدّعي أنَّ الحاسوب المُستهدَف استُعْمِلَ في أنشطة غير قانونيَّة؛ منها تحميل برامج غير مُرخَّصة، ومن أجل هذا سُمِّي «حصان طروادة الشُّرطة».

وبعد إخبار المُسْتَخْدِم بذلك، يُرسل التَّحذير رسالة مُقايَضة لدَفْع غرامة باستعمال قسيمة مُسبَقة الدَّفع من خدمة دَفْع تُخْفِي الهُوِيَّة مثل يوكاش أو بيسيفكارد لكي يعمل النِّظام، ولإحكام الاستهداف يظهر البرنامج الخبيث على شاشة الجهاز المُستهدَف التي تُظْهِر عنوان الأي بي IP للحاسوب، وكذلك بعض نُسَخ لقطات من الكاميرا لتُوهِم المُسْتَخْدِم أنَّه مُلاحَق.

وانتشر «Reveton» في عدَّة دُوَل أوروبيَّة في أوائل عام 2012م، وتنوَّعت نُسَخ البرنامج بتنوُّع شعارات مُنظَّمات تطبيق القانون في كُلّ بلد.

وفي أغسطس عام 2012م، بدأت نُسْخَة جديدة من «Reveton» تَنْتشر في الولايات المتَّحدة، وتدّعي أنَّها تطلب غرامة 200 دولار أمريكيّ لمكتب التَّحقيقات الفدراليّ من خلال بطاقة منيباك.

وفي فبراير عام 2013م، اعتقلت السُّلطات الإسبانيَّة مُواطنًا روسيًّا في دبي؛ لارتباطه بشبكة جريمة تَستعمل البرمجيَّة الخبيث «Reveton»، كما اعتُقِلَ 10 آخرون في أغسطس عام 2014م.

1. من دودة موريس إلى استهداف المنشآت.. تعرف على الأجيال الخمسة للتَّهديدات السّيبرانيَّة، الجزيرة، 15 ديسمبر 2019م، مُتَاح على الرَّابط: https://cutt.us/1B445
2. Lessing, Marlese. (2020). Case Study: Reveton Ransomware, SDXCENTRAL, on site: https://cutt.us/2IICN

المثال الرَّابع: ريجن Regin [1]

ريجـن (Regin) هـي برمجيَّـة خبيثـة مُتطـوِّرة كُشِـفَ عنهـا فـي نوفمبـر عـام 2014م، وتَستهدف الذيـن يستخدمون أجهـزة الحاسـوب القائمـة على نظـام مايكروسـوفت ويـندوز.

وتسبَّبت في إصابة العديد من الأجهزة في العالَم:

- 28 % في روسيا.
- 24 % في المملكة العربيَّة السعوديَّة.
- 9 % في كُلّ من المكسيك وأيرلندا.
- 5 % في كُلّ من الهند، أفغانستان، إيران، بلجيكا، النمسا وباكستان.

والضحايـا الرَّئيسـيُّون لهـذه البرمجيَّـة الخبيثـة هـم مـن الأفـراد العاديّيـن والشَّـركات الصَّغيـرة وشـركات الاتِّصـالات.

المثال الخامس: قائمة بكلمات المرور المُعرَّضة للاختراق

نشَـر فريـقٌ مـن الباحثيـن مـن «Nord Pass» تحذيـرًا للمُسْـتَخْدِمِين؛ للتَّحقُّـق مـن إعداداتهـم، والسَّـبب اسـتخدام كلمـات مـرور معروفـة مثـل:

" 123456 "، " password "، " qwerty ".

1. Het Regin-platform, Kaspersky, on site: https://cutt.us/nYOFi

وفيما يلي أهمّ 10 كلمات مرور شائعة في جميع أنحاء العالَم:

- dolphin
- 123456
- 123456789
- 111111
- 12345
- 12345678
- password
- Qwerty
- 1234567
- 123123

وكلَّما كانت كلمة المرور الخاصَّة بك تُشبه أنماط الكلمات العاديَّة؛ طالت المدَّة التي تستغرقها أداة التّكرار لتَخْمينها.

وهناك صِيَغ كلمات المرور التي يَصْعُب تخمينها تطبيقًا على المثال السابق، مثل:

- Cat.lov3r
- CAt.lov3r
- !! i7ovemyCat
- C0tsaremybestfr13nds
- sn00pdoggycat

تمارين وتَدْريبَات

تُعدّ التَّمارِين جزءًا رئيسًا من عمليَّة التَّدريب، وهي تُحقِّق عدَّة أهداف وغايات، فيما يلي تبيان لأهمّها:

- التَّمارِين أداة فعَّالة لمعرفة مدى استفادة الطَّلبة من المحتوى التَّدريبيّ، ومدى الأثر الذي حقَّقته على المخزون المعرفيّ لدى الطَّلبة.
- أداة مُهمَّة لترسيخ المعلومات والمعارف لدى الطَّلبة؛ كونها تُمثِّل مُراجَعَة سريعة للمحتوى التَّدريبيّ.
- اكتشاف الفُرُوق المعرفيَّة بين الطَّلبة.
- تُمثِّل تغذيةً عكسيَّة للمُدرِّب، وتُقدِّم له معلومات حول فاعليَّة الحقيبة التَّدريبيَّة وفاعليَّة أسلوبه التَّدريبيّ.

منهجيَّة التَّعامُل مع التَّمارِين

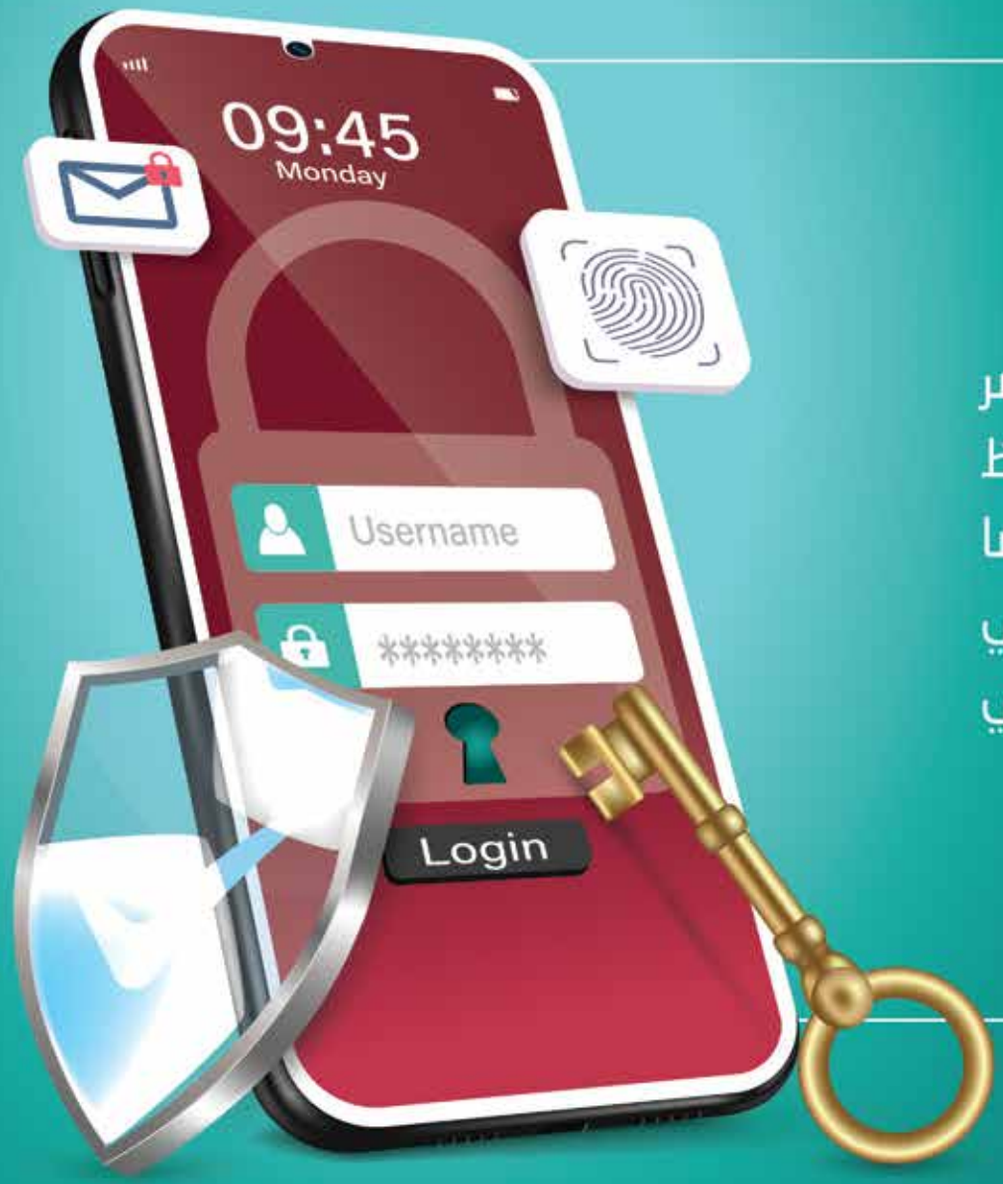
التَّمارِين المذكورة في هذا القسم شاملة للمحتوى التَّدريبيّ في هذه الحقيبة، وفيما يلي توضيح للمنهجيَّة المُقترَحَة للتَّعامُل معها:

- خلال التَّدريب يقوم المُدرِّب وبعد الانتهاء من فِكْرةٍ ما بالطَّلب من الطَّلبة فَتْح الكُتَيِّب الخاصّ بهم، والقيام بالإجابة عن السُّؤال المُحدَّد، والذي يرتبط بشكلٍ مُباشِر بالفكرة أو الموضوع الذي يُقدِّمه لهم.
- التَّمارِين مُختَارة بعناية، بحيث تكون مُبسَّطة وسهلة الفَهْم، وقابلة للحلّ مِن قِبَل طلبة المرحلة الابتدائيَّة، وهنا من الممكن للمُدرِّب تقديم الدَّعْم للطَّلبة في الإجابة عن بعض التَّمارِين في حال اقتضت الضَّرورة، وهذا الأمر يُتْرَك لتَقْدير المُدرِّب.
- التَّمارِين ستكون على جزأين؛ جزءٌ خاصّ بالصَّفّ، ويُسمَّى التَّمارِين الصَّفِّيَّة، وآخر لا صفِّيّ، ويقوم الطَّالب بالإجابة عنها كواجبٍ منزليّ.
- تمَّ إضافَة الحَلّ الخاصّ بكُلّ تَمْرين، مع تمييز الإجَابَة بلَوْن مُختَلف.

وفيما يلي تبيان للتَّمارين الخاصَّة بطلبة المرحلة الابتدائيَّة، مُرتَّبة وفقًا لطبيعتها الصَّفِّيَّة واللَّاصَفِّيَّة، مع العِلْم أنَّ ذات التَّمارِين وبصيغتها الموجودة هنا موجودة في الكُتَيِّب الخاص بالطَّالب.

أولًا: التَّمَارين الصَّفِّيَّة

التَّدريبات هنا مَرْفَقَة بالحَلّ، بينما في كُتَيِّب الطَّالِب مَكْتُوبة بدون حَلّ، ومَرْفَق معها توجيه للطَّالب لكيفيَّة الحلّ، وذلك حيث تقتضي الضَّرورة.

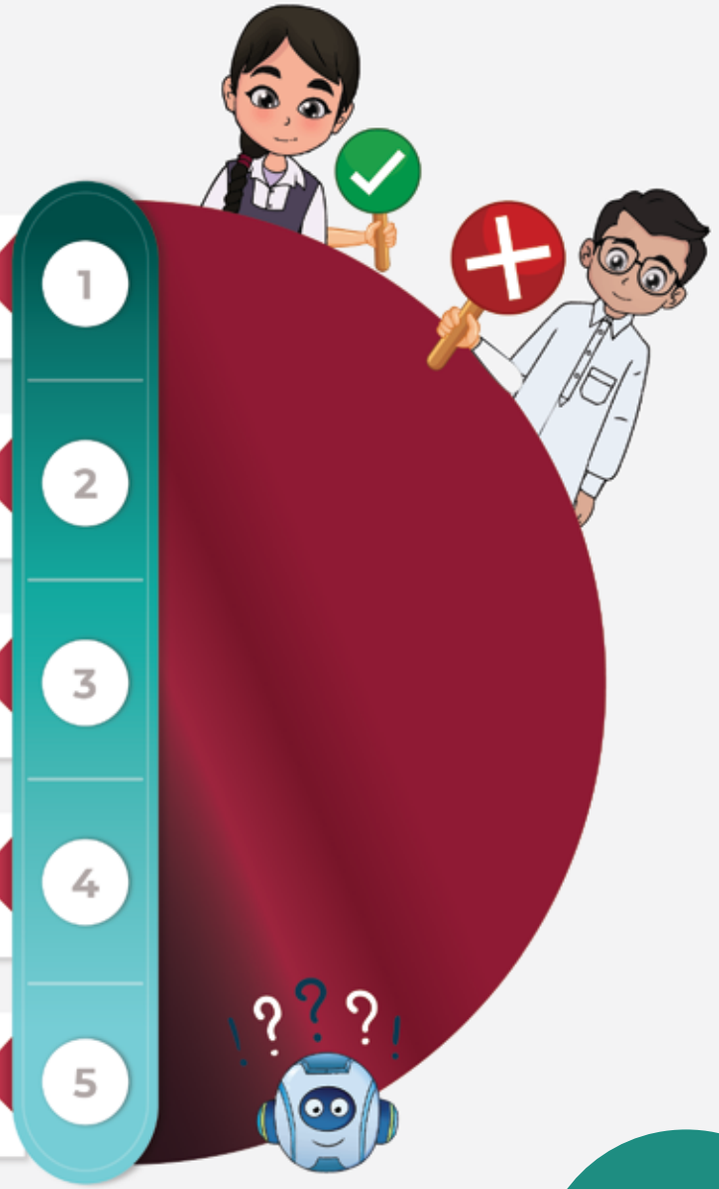


هل تعلم؟

الأَمْن السّيبرانيّ لا تَقتصر مَهمّته فقط على الحِفَاظ على البيانات، بل يساعد أيضًا في استرجاع البيانات التي تمّت سَرقتها وتَسريبها في أسرع وقتٍ.

التَّمرين الأَوَّل

ضَعْ علامة (✓) أمام العبارة الصحيحة، أو علامة (✗) أمام العبارة الخاطئة:



1. الأَمْن السّـيبرانيّ هو حمـــاية الأجهـزة والشَّبكات والتَّطبيقات من المَخاطِر الرَّقميَّة. ✓
2. لا تتحمَّـــل المُؤسَّسَـات مسـؤوليَّة تـأمين البيانات الخاصَّة بها أو بالعملاء المُتعامِلين معها. ✗
3. حماية البيانات تَخْلق ثقةً بين المُؤسَّسَة والعملاء المُتعامِلين معها. ✓
4. لا بُدَّ من اتِّخاذ تدابير وأدوات مُتخَصِّصة من أجل حماية البيانات خاصَّة غير المُصَرَّح بالوصول إليها. ✓
5. يحتاج الأفراد إلى معرفة أُسُس الأمـان الرَّقميّ لحمـــاية أنفسهم وبياناتهم الخاصَّة من المَخاطِر السّيبرانيَّة. ✓

6 ازداد الاهتمـام بالأَمْن السّـيبرانيّ بعد اعتـماد أغلب المُؤسّـسَات والحكومات على الخِدْمَات الرّقميّة والإلكترونيّة.

7 خَرْق الخصوصيّة وسـرقة البيانات مشـكلة سَـهْلة لا عَواقِب كبيرة لها.

8 الهجمات الإلكترونية لها الكثير من الفوائد.

9 يمكن للهجمات الإلكترونية أن تكشف البيانات السّرّيّة أو تَتَسبّب في سرقتها أو حَذْفها بشكلٍ مُتعمّد.

10 لا تَحْدُث الهجمات الإلكترونية بشـكلٍ مُتَعَمّد، ويمكن لأيّ شخص القيام بها.


PASSWORD PROTECTED
انْتَبِه!
وضع كلمة سرّ واحدة لجميع الحسابات الشَّخصيَّة والبريد الإلكتروني، يزيد من فُرَص خرق أجهــزتك الإلكترونيّة.
* * * * *


01001110
01110100
0111011101
111100010110

هل تعلم؟

مخترقو الأجهزة والبيانات (الهاكرز) يبحثون عن الثّغرات التي يمكن من خلالها سرقة الأموال والمعلومات الخاصّة، ولتفادي ذلك ينبغي تحديث البرامج واستخدام كلمات مرور قويّة وتغييرها بين الحين والآخر، وتشفير البيانات المُهمّة.

التَّمْرين الثَّاني

صِلْ بين العِبَارَات في العمود الأوّل
مع ما يَنْسَجم معها في العَمُود الثَّاني

الجلوس لأوقات طويلة على الإنترنت	يُؤدّي إلى العُزْلة الاجتماعيَّة.
استخدام الإنترنت لأوقاتٍ طويلةٍ يمكن أن يصيبك	بالاكتئاب ونَوْبات القلق والتَّوتُّر.
قد تتعرَّض لخرق الخصوصية من خلال	محاولات القَرْصَنة وسرقة البيانات عبر المواقع الإلكترونيَّة.
خرق الخصوصية	من الجرائم التي يُعاقِب عليها القانون.
التَّعرُّض للمحتوى العَنِيف وغير المَناسِب للأطفال	يُؤدّي إلى مشكلات أخلاقيَّة ونفسيَّة وعضويَّة.
يمكنك أن تُصَاب بإدمان الإنترنت	حين تجلس لفترات طويلة على الإنترنت دون تعامُل مع الآخرين.
يُهدِّد الإنترنت أمان المجتمع	لأنَّ بعض الجماعات الإرهابيَّة تلجأ إليه لتجنيد الشَّباب والإضرار بالمجتمع.
يُهدِّد الإنترنت الثَّقافة الوطنيَّة	لأنَّ الانفتاح على الثَّقافات الأخرى بدون ضوابط قد يُؤدّي إلى اكتساب ما هو غير مُناسِب لثقافتنا، ويتنافَى مع مُعتقداتنا الدِّينيَّة والثَّقافيَّة.

انْتَبِه!

تجاهُل إعدادات الخصوصيّة،
وعدم مُتابَعة أحدث التّغييرات
بنُظُم التّشْغيل يعرِّض بياناتك
لخَطَر الاختراق.

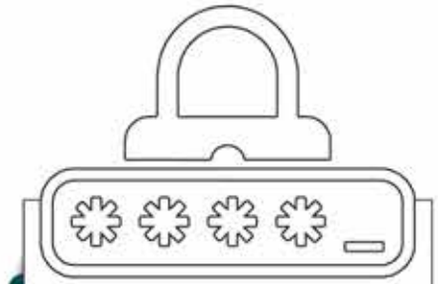
التَّمْرين الثَّالث

اقرأ الكلمات التَّالية بِتَمَعُّنٍ، وأيّ شيءٍ مما يلي يمكن سرقته عن طريق الإنترنت لَوِّنه بأحد الألوان.

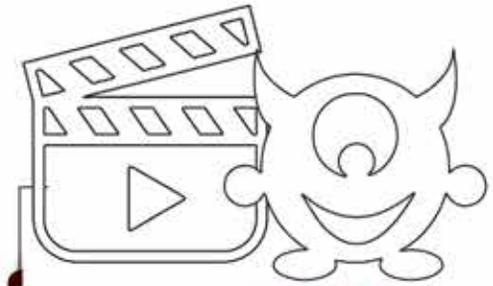
المعلـومـات والمسـتنـدات الموجودة على الحاسب الآليّ

أرقام الحسابات المصرفيّة

أرقام بطاقات الائتمان



كلمات المرور



ملفّات أفلام الكارتون

بيانات الأوراق الرّسميّة مثل الرُّخصة وجواز السّفر


مواعيد العمل
المنشورات على منصّات التّواصل الاجتماعيّ
الأكواد المصدريّة والخوارزميّات
ملفّات الأغاني
الكُتب الرّقميّة
بيانات الحسابات على منصّات التّواصل الاجتماعيّ


الصُّوَر والمَقاطِع
المَصوّرة الخاصّة


أسماء وقوائم العُمَلاء


الهَوِيّات الإلكترونيّة

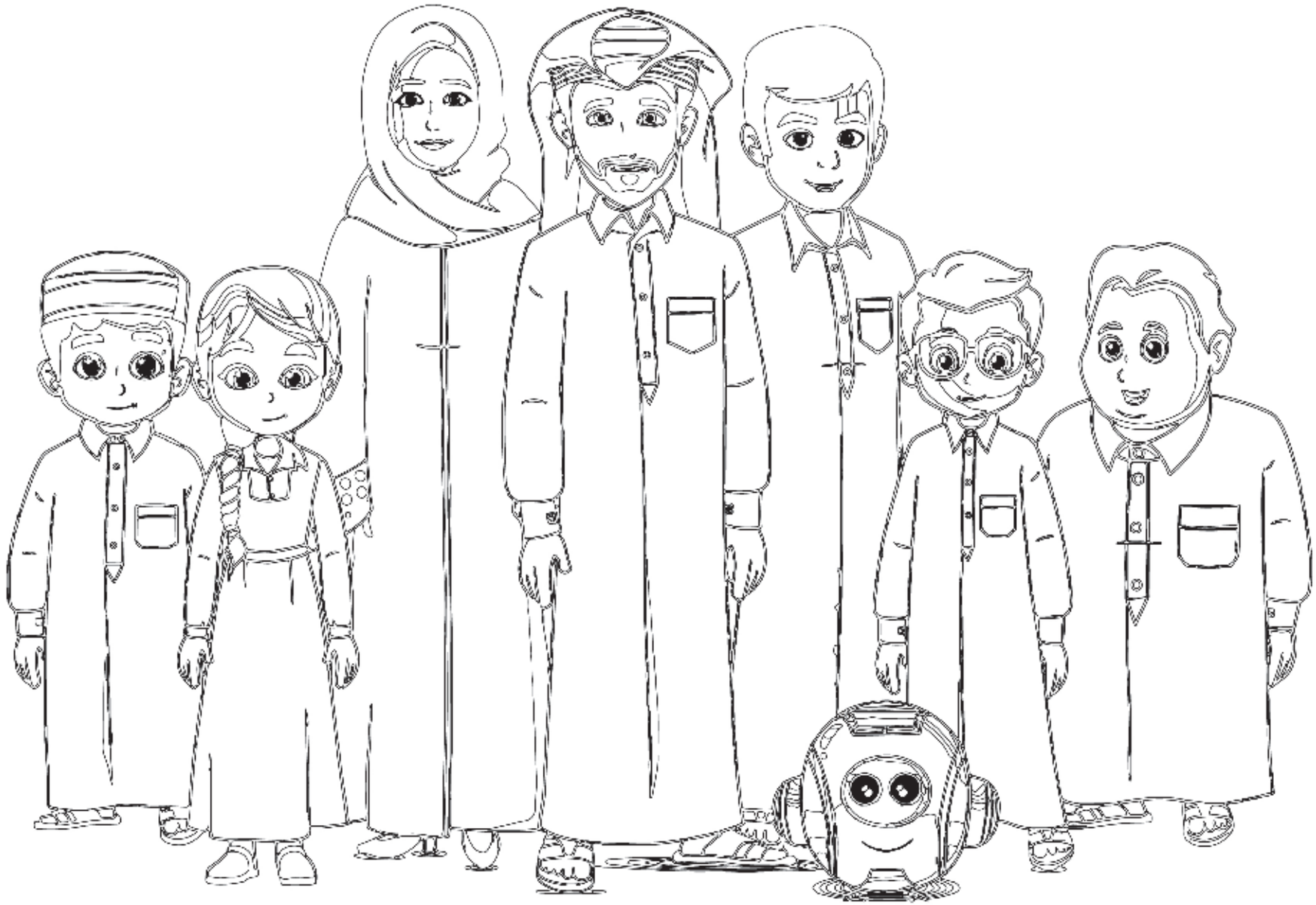

التّطبيقات


السّجلات الطّبيّة


سجلات الموارد البشريّة
وبيانات المُوظّفين

انْتَبِه!

عدم تحديث أنظمة الأجهزة الذَّكيَّة؛ سواءً أجهزة الحاسوب الشخصي أو الهواتف، يُعرّضها لعَشَرات الثّغرَات التي يَسْتَغِلُّها مخترقو الأجهزة لسَرقة البيانات وخرق الأجهزة.



التَّمْرين الرابع

اقرأ الكلمات الوَارِدَة بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هذه الكلمات تُعَبِّر عن **الآثار والمخاطر الرقمية**؛ وقم بتلوين المَرَبَّع الذي به الكلمة أو العبارة.

القلَق

التَّوتُّر

تشتُّت الانتباه

السَّعادَة

الفَخْر

القُدْرَة على المَواجَهة

تجنُّب الأصدِقاء

الرَّغْبَة في تَرْك المدرسة

مشكلات النَّوْم

فَقْد احترام الذَّات

تناقُص العَلامَات الدِّراسيَّة

زيادة الصَّداقات

فُقْدان الطَّاقة

المَشْكِلات النَّفسيَّة

الخوف من المَواجَهَة

فَقْدان الثِّقة بالنَّفس

التَّعاسَة

الرَّغْبَة في القيام بالأنْشِطَة

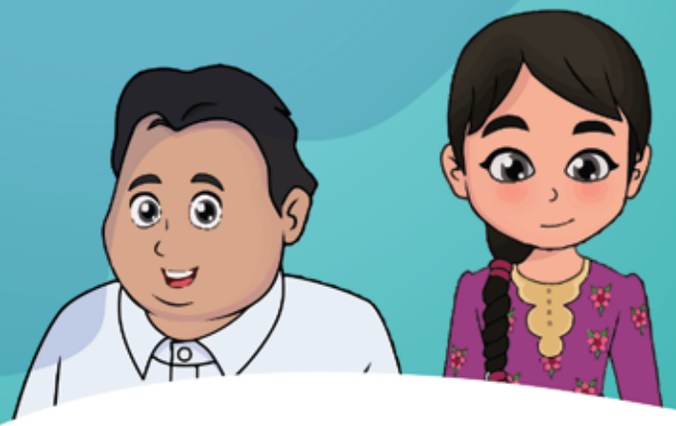
تجنُّب الخروج

التَّركيز

زيادة الوَزْن

هل تعلم؟

كثرة الإعلانات تُعدّ مؤشّرًا على وجود الفيروسات على مواقع الويب، والتي تنتقل إلى الأجهزة الإلكترونيّة بمجرد الضَّغْط عليها.



التَّمْرين الخامس

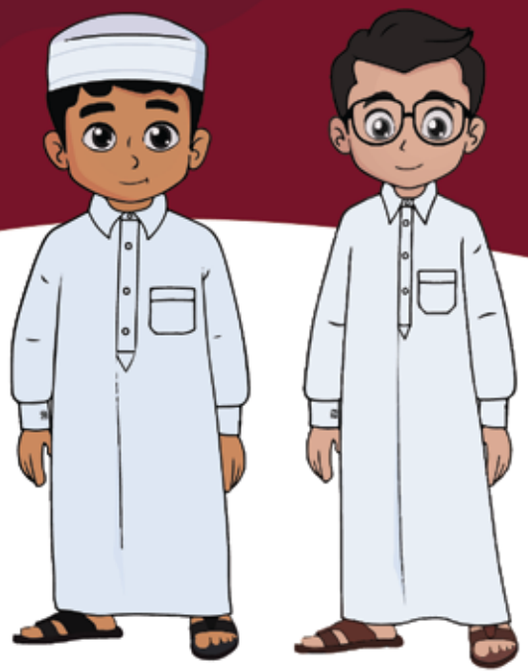
اقرأ كلمات المرور الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، وفَكِّر فيما إذا كانت هذه الكلمات تُعَدّ **كلمات مرور قويّة أم لا**.

- [ ] Medo123
- [ ] Password
- [ ] 123456
- [ ] 654321
- [ ] Penten
- [x] Me@12do
- [x] 2020MMeeDDoo$%
- [ ] 123medo
- [ ] Pass123
- [ ] Klmetser

انْتَبِه! الضَّغْط على أيّ رابط غير معروف أو مشكوك فيه، يتسبَّب في خرق الحسابات الشخصية.

التَّمْرين السَّادس

اختر الإجابة الصحيحة فيما يلي:



1. **حين أتَعَرَّض لجريمةٍ إلكترونيَّة عليَّ أن:**

- [ ] أسكت تمامًا ولا أُخْبِر أيّ أحدٍ.
- [ ] أتواصَل مع الشُّرطة دون عِلْم والدي ووالدتي.
- [x] أتَوجَّه فَوْرًا إلى أحد والديَّ أو إلى مُعلِّمي في المدرسة.

2. **حين أتعرَّض لجريمة الابتزاز الإلكترونيّ،**

أوَّل شيءٍ يجب عليَّ، أن:

- [ ] أُهدِّد مَن يقوم بابتزازي وأستفزّه.
- [x] أحظُره تمامًا، وأُبَلِّغ عنه مُقدِّمي الخدمة.
- [ ] أُحاول إعطاءَه ما يُريد؛ كي لا يَضُرّني بما يَعْرفه عنّي.

3. **لحماية نفسي على شبكة الإنترنت عليَّ:**

- [ ] أنْ أُخْبِر الجميع كلّ شيءٍ عنّي.
- [ ] ألّا أُكَوِّن أيّ صَداقات علَى الإنترنت مطلقًا.
- [x] أنْ أُشارك المعلومات العاديَّة وغير الخاصَّة، والتي لا يمكن أن يَستغلّها أحدٌ ضدّي.


ثانيًا: التَّمارين اللَّاصَفِّيَّة

انْتَبِه!

مُشارَكة الكثير من التّفاصيل عن الحياة الشّخصيّة، وطبيعة عملنا ومنزلنا على الإنترنت تُعرّضنا للخرق والسّـرِقة.

التَّمْرين الأوَّل

استخـرِج الكلمـات التّالية من الجـدول:

اقرأ الكلمات الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، وابحثْ في الخانات عن حُرُوف مُتتالية تُشَكِّل هذه الكلمات.

ا	ل	أ	م	ن	ا	ل	س	ي	ب	ر	ا	ن	ي
ل	ص	غ	ش	ب	ذ	خ	د	م	ا	ت	س	س	ي
ج	و	و	ك	ا	ر	ث	ة	ا	ل	س	ر	ي	ة
ر	ص	ك	ل		ا	ل	ه	ج	م	ا	ت	ر	ذ
ي	غ	ش	ة	ا	ل	م	خ	ا	ط	ر	ل	ا	ف
م	ا	ل	ا	ح	ت	ي	ا	ل		س	ر	ق	ة
ة	ح	م	ا	ي	ة	ا	ل	ب	ي	ا	ن	ا	ت
ا	ل	أ	م	ا	ن	ا	ل	ر	ق	م	ي	ع	ة

الأَمْن السّيبرانيّ - لصوص - الأمان الرّقميّ - الهجمات - الجريمة - البيانات - السّرّيّة - المَخَاطِر

الاحتيال - خِدْمات - سرقة - مشكلة - حماية - كارثة

التَّمْرين الثَّاني

اقرأ العبارات الوَارِدَة أَدْنَاهُ بِتَمَعُّنٍ، واقرأ الكلمات أو العبارات الوَارِدَة بين إشارَتَي التَّنصيص "..." ، وحَدِّد الكلمة المُناسِبَة

- الإنترنت شبكة " ☑ **دوليّة** ☐ **محليّة**".
- الإنترنت وسيلة " ☑ **للتَّعلُّم والتَّرفيه** ☐ **للتَّرفيه والتَّسلية**".
- الإنترنت مَهِمّ لنَقْل ومُشارَكة " ☐ **البيانات** ☑ **الأفلام والمسلسلات**".
- هناك ارتباط بين الإصابة بـ " ☐ **النّحافة** ☑ **السّمنة**" وبين استخدام الإنترنت لوقتٍ طويلٍ.
- استخدام الإنترنت لوقتٍ طويلٍ قد يتسبَّب في جعلك "☑ **منعزلًا اجتماعيًّا** ☐ **اجتماعيًّا ومُحِبًّا للتَّجمُّعات**".
- هناك أبحاث تُؤكِّد أنَّ استخدام الإنترنت لوقتٍ طويلٍ قد يُصيبك بالكثير من" ☐ **الترقيات** ☑ **الأمراض**" الجسديَّة والنفسيَّة.

- الإنترنت مليء بـ "☑ **الفوائد والمَخَاطِر** ☐ **المَخَاطِر فقط**".
- تَسْتَغِلّ الجماعات الإرهابيَّة الإنترنت لـ "☐ **تعليم** ☑ **تجنيد**" الشَّباب.
- سرقة البيانات وخرق الحسابات الشَّخصيَّة "☑ **جريمة** ☐ **جائزة**" في القانون.
- من أبرز مشكلات الإنترنت أنَّ كلّ البيانات مُعرَّضة "☐ **للحفظ** ☑ **للسَّرقة والخَرْق**".
- إدمان الإنترنت قد يُؤثِّر على قُدْرتك على "☑ **التَّفَاعُل والتَّعامُل** ☐ **الحُضُور**" مع الآخرين.
- التَّعرُّض لثقافات جديدة قد يُؤدّي إلى "☐ **رفض** ☑ **اكتساب**" عادات تُخالِف معتقداتنا وقِيَمنا.
- يُهدِّد الإنترنت الثَّقافة المجتمعيَّة بسبب "☐ **انغلاقه** ☑ **انفتاحه**" على العالَم وثقافاته المختلفة.
- الأطفال هم الأكثر عُرْضَة للمشكلات على شبكة الإنترنت بسبب المحتوى "☑ **العنيف** ☐ **الموسيقي**".
- إدمان الإنترنت من المَشكلات الشَّائعة والتي تَحْدُث بسبب

"☑ **اســتخدام الإنترنت لـــــــوقتٍ طويـــلٍ** ☐ **اســتـــــخدام الإنترنت لمدة ســاعتين كلّ يوم**".

التَّمْرين الثَّالث

اقرأ الجُمَل الوَارِدَة في الجدول بِتَمَعُّنٍ، وفَكِّر إذا كانت المعلومات **صحيحة أم خاطئة**.

يمكن للمُخْتَرِقِينَ سَرِقَة البيانات الخاصَّة بالمُستخْدِمِين من خلال الاحتيال والتَّظَاهُر بأنَّهم جهة موثوقة، مثل البنوك أو شركات الاتِّصالات.	صحيحة	
كلمات المرور الضَّعيفة قد تكون أسْهل طَريقة لسَرقة البيانات.	صحيحة	
أحيانًا يُرْسِل المُخْتَرِق ملفًّا أو رابطًا عبر البريد الإلكترونيّ بمُجَرَّد الضَّغْط عليه يَتِمّ خرق الجهاز بكلّ سهولةٍ وسرقة البيانات.	صحيحة	
لا مُشكلة من سَرِقة البيانات.	خاطئة	
لا يمكن للمُخْتَرِق الاستفادة من البيانات التي قام بسَرِقتها.	خاطئة	
عليك اختيار كلمات سِرّ بسيطة، ويمكن تخمينها بسهولة.	خاطئة	

لا بُدَّ أن تتأكَّد أنَّه لا تُوجد ثَغرَات أمنيَّة في نظام حاسوبك أو تطبيقات مُختَرَقَة على هاتفك لتَجَنُّب خَطَر سرقة البيانات.	صحيحة
لا يَحْدُث أيّ خطأ بشريّ يمكن أن يُؤدّي إلى سرقة البيانات.	خاطئة
التَّنزيلات دائمًا آمِنَة، ولا يمكن خرق الأجهزة أو سرقة البيانات من خلالها.	خاطئة
يمكن أن تتسبَّب المشكلات في قواعد البيانات أو الخوادم في سرقة البيانات وسهولة دُخُول المُخْتَرِقِين إلى الشَّبكات أو الأجهزة.	صحيحة
قد يتسبَّب الشَّخْص نفسه في سرقة بياناته دون أن يَشْعُر، فقط بالإفصاح عن كثير من المعلومات من خلال مِنَصَّات التَّواصُل الاجتماعيّ.	صحيحة
أحيانًا تتسبَّب سرقة الهواتف أو أجهزة الحاسوب في تسريب البيانات.	صحيحة
استخدام شبكات Wi-Fi (الإنترنت) العامَّة، أو أجهزة الحاسوب في الأماكن العامَّة مثل المكتبات قد يُعرِّض البيانات لخطر السَّرقة.	صحيحة
لا تحتاج الشركات أو المُؤسَّسَات إلى تأمين قواعد البيانات أو الخوادم من أجل حماية بيانات العملاء.	خاطئة

التَّمْرين الرَّابع

لَوِّن الصُّورَة التَّالية

التَّمْرين الخامس

ضع علامة (✓) أمام العِبَارات التي يمكـــن أن تُســـاعِدَك فـــي كتـــابة **كلمة مرور قويَّة.**

أسْتَخْدم نفس حُرُوف اسم المُستَخْدِم.	
أسْتَخْدم مجموعةً مُتَنَوِّعَة من الحروف والأرقام.	✓
أستَخْدم تاريخ يوم ميلاديّ.	
أسْتَخْدم مجموعةً من الحروف الكبيرة والصَّغيرة وبعض الرُّموز.	✓
أسْتَخْدم كلمةً لا يُمْكِنُني تَذكُّرها.	
أسْتَخْدم كلمةً قريبةً من كلمات المرور القديمة.	
أسْتَخْدِم كلمةَ password .	
أسْتَخْدِم اسم قطتي / كلبي.	
أسْتَخْدم تاريخًا مُمَيَّزًا بالنِّسبة لي.	
أسْتَخْدم كلمة يَسْهُل عليَّ تَذَكُّرها، ويصعب على الآخرين تَخْمينها.	✓

انْتَبِه!

قبول طلبات الصَّداقة من أشخاص مجهولين أمرٌ خطيرٌ؛ لأنَّه يُتيح لهم خرق خصوصيتك ومعرفة معلوماتك الشَّخصيَّة.


الألعاب التّدْريبيّة

نَاقِشْ مع زُمَلائك الأسئلة التَّالية

01 الأمن السّيبرانيّ cyber security يُطلق عليه أيضًا

(أمن الحاسوب) (عدد الحروف 10)

02 طول كلمة المرور القويّة

(12 حرفًا) (عدد الحروف 6)

03 أشخاص يُسبّبون ضررًا بالغًا في أجهزتنا الإلكترونيّة

(الهاكرز) (عدد الحروف 7)

04 أحد أنواع الأمن السّيبرانيّ

(الأمن السّحابيّ) (عدد الحروف 12)

05 أحد أمثلة الحقوق الفكريّة

(العلامة التّجاريّة) (عدد الحروف 15)

ضَع المُسمَّى المُناسِـــــب

تحتوي على روابط أو ملفَّات بها فيروسات أو برمجيَّات خبيثة، وبمُجَرَّد فَتْحها أو النَّقْر عليها تَسْرق بياناتك... ما هي؟

الرَّسائل الوَهْميَّة.

بمُجرَّد قَبُولك لها فإنَّ خصوصيّتك ومعلوماتك الشَّخصيَّة تُصبح مُهدَّدة... ما هي؟

طلبات الصَّداقَة على مواقع التَّواصُل الاجتماعيّ.

مَهمّته هي حماية نُظُم التَّشْغيل المعلوماتيَّة ومُكوّناتها من أجهزة وخِدْمَات وبيانات... ما هو هذا الشَّيء؟

الأَمْن السّيبرانيّ.

شَكْل مُتطوّر من أشكال الجريمة العَابِرة للحدود، التي تحدث في مجال الفضاء الإلكترونيّ.

الجريمة الإلكترونيَّة.

نَشْر أكاذيب أو صُوَر مُحْرِجَة لشخصٍ ما، أو إرسال رسائل مُؤذية، أو تهديد لشخصٍ ما على وسائل التَّواصُل الاجتماعيّ، كلّها صُوَر من

التَّنَمُّر عبر الإنترنت.

تتألَّف كلمة المرورالقويَّة من

مجموعة من الأحرف والأرقام والرُّموز.

مشروع التَّخرُّج

مشروع التَّخرُّج هو واجبٌ تقوم به بمُفْرَدك أو بالاشتراك مع زميل أو زميلين من زُمَلائك، تقوم من خلاله وتحت إشراف المُدرِّب بأحد الواجبات التَّالية:

كتابة قِصَّة قصيرة عن شَخْصٍ ما تعرَّض لأحد المَخاطِر الرَّقميَّة، (تختار أنت هذه المَخاطِر)، وتُبَيِّن كيف تَصرَّف بحكمةٍ، وتَمكَّن من مُواجَهة هذه المَخاطِر، وما هي الإجراءات التي قام بها.

تَخيَّل نَفْسَك أنَّكَ مُدرِّب، وستقوم بكتابة بعض التَّوجيهات للطَّلَبَة تُبَيِّن لهم فيها كيف يَقُومون بحماية أنفسهم من المَخاطِر الرَّقميَّة.

مراجـــــــع

المحتوى العلمي

في الحـــــــقيبة

المراجع العربيَّة:

1. العتيبـي ميعـاد (2017م) أساسـيَّات فـي الأَمْـن السّـيبرانيّ، مُتَـاح علَـى الرَّابـط: https://www.docdroid.net/1BTYYas/asasyat-fy-alamn-al-sybrany-pdf

2. مـن دودة موريـس إلـى اسـتهداف المنشـآت.. تعـرَّف علـى الأجيـال الخمسـة للتَّهديـدات السـيبرانيَّة، الجزيـرة، 15 ديسـمبر 2019م، مُتَـاح علَـى الرَّابـط: https://cutt.us/1B445

3. يوسـف، أميـر. (2015م). جرائـم تقنيـة المعلومـات بـدُوَل الخليـج العربـيّ، والجهـود الدّوليَّـة والمحلِّيَّـة لمكافحتـه، جرائـم الإنترنـت والحاسـوب الإلكترونيَّـة فـي دُوَل الخليـج العربـيّ. مصـر: دار الكتـب العربيـة. ص 68-74.

المراجع الأجنبيَّة:

1. Het Regin-platform, Kaspersky, on site: https://cutt.us/nYOFi

2. Lessing, Marlese. (2020). Case Study: Reveton Ransomware, SDXCENTRAL, on site: https://cutt.us/2IICN

3. Melissa Virus, FBI, on site: https://cutt.us/m1J9f

4. Person, Tim, P. and Jordan, T. (2017) A sociology of hackers: 10: Cyberspace crime: Tim Jordan, Paul Tayl, Taylor & Francis. On site: https://cutt.us/NwnyZ

5. Sarker, I.H. and Kayes, A.S.M. (2020) Cybersecurity Data Science: An overview from machine learning perspective - journal of big data, SpringerLink. On site: https://link.springer.com/article/10.1186/s40537-020-00318-5

6. Smith, A.D. and Rupp, W.T. (2002), «Issues in cybersecurity; understanding the potential risks associated with hackers/crackers», Information Management & Computer Security, Vol. 10 No. 4, pp. 178-183.

7. yagibca, prateekt (2023) Cyber Security, types and importance, GeeksforGeeks. On site: https://www.geeksforgeeks.org/cyber security-types-and-importance/


CyberEco


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency