CyberEco

مقا لدعم السلامة الرقمية

Together to support digital safety

حمـاية الأجـهزة الإلكترونيّة ومُواجَـهة الاختراقات الأمنيّة

محتوى تدريبيّ موجّه لأولياء الأمور

حقيبة خاصّة بالمُدرّب

الوكالة الوطنية للامن السيبيراني

National Cyber Security Agency

حماية الأجهزة الإلكترونيَّة ومُواجَهة الاختراقات الأمنيَّة

مُحتوى تدريبيّ موجَّه لأولياء الأمور

المادَّة التَّدريبيَّة

(حَقيبَة 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 الحقيبة التَّدريبيَّة على تزويد المُدرِّب بأدوات ووسائل تدريبيَّة؛ بحيث يَسْهُل عليه تقديم المعلومات للمُتدرِّبين، وتُعدّ هذه الحقيبة مُوجِّهًا عامًّا للمُدرِّب ودَاعِمًا له، إضافةً إلى تزويد المُدرِّب بأدواتٍ ووسائل تدريب تدعمه في عمليَّة التَّدريب.

أهداف الحَقيبَة التَّدْريبيَّة

- تزويد المُدرِّب بوسائل تدريب تُساعِده على إيصال المحتوى التَّدريبيّ للمُتدرِّبين.
- تقديم المعلومات والمحتوى التَّدريبيّ بشكلٍ سَهْل ومُبسَّط.
- تقديم المحتوى التَّدريبيّ الخاصّ بحماية الأجهزة الإلكترونيَّة، مُرفَقًا بأدوات ووسائل تدريب متعدِّدة.

محتوى الحَقيبَة التَّدْريبيَّة

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

1. **ملفّ العَرْض.**
2. **فيديوهات تدريبيَّة.**
3. **بطاقات تدريبيَّة،** وهي على شَكْل معلومات عامَّة مرفقة بصور تعبيريَّة، يَعْرضها المُدرِّب على المُتدرِّبين.
4. **إسكتشات،** تتضمَّن معلومات حول المَحاوِر الرَّئيسة في المُحتَوى التَّدريبيّ.

المحتوى العِلْميّ للحَقيبَة التَّدريبيَّة

الجَدْوَل الزَّمنيّ للورشة

المحتوى	الوقت المُخصَّص
مُقدِّمة عامَّة	10 دقائق
الجانب النَّظريّ من المادَّة	30 دقيقة
عَرْض الفيديوهات التَّدريبيَّة	30 دقيقة
استراحة قصيرة	20 دقيقة
حِوار ونقاش مع المُتدرِّبين	30 دقيقة
المدَّة الزَّمنيَّة للورشة	ساعتان

دليل إرشادي للمُدَرِّب

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

- المحتوى العِلْمِيّ قد يتضمَّن مفاهيم خارج اختصاص المُتدرِّبين، لذلك لا بُدّ للمُدرِّب من تقديم المعلومات بشكلٍ مُبسَّطٍ.
- يَعْرض المُدرِّب شرائح العَرْض عند كُلّ نقطة يتحدَّث عنها، فمثلًا عند الحديث عن مفهوم حماية الأجهزة الإلكترونيَّة يتمّ عَرْض الشَّريحة التي تتناول ذات المفهوم.
- يَعرِض المُدَرِّب الجزء الخاص بـ"إسكتشات" أثناء قيام الطَّلبة بحل التَّمارين والتَّدريبات.
- في أثناء عَرْض المادَّة العِلْمِيَّة لكلّ فَصْل يتمّ استقطاع فترة من الوقت المُخصَّص له لعَرْض عددٍ من الرَّوابط ذات الصِّلة بمضمون الفَصْل.
- يَعْرض المُدرِّب الفيديوهات -المذكورة في ملفٍّ منفصل- على أولياء أمور الطَّلبَة في نهاية كلّ فَصْل، أو في المَوْضع الذي يراه مناسبًا.
- يُرْجى فَتْح باب المناقشة مع أولياء أمور الطَّلبَة في المواضع التي يراها المُدرِّب مناسبة.

ثانيًا: المادَّة العِلْمِيَّة

مُقدِّمة

إنّ حماية الأجهزة الإلكترونيَّة والشَّبكات ومن ثمّ حماية المعلومات والبيانات من الانتهاك والإتلاف من المهامّ التي يقوم بها الأمن السِّيبرانيّ سواءٌ بالنِّسبة للأفراد أو المؤسَّسات، وقد دخل الأمن السِّيبرانيّ في عدد من المجالات المختلفة التي يُوفِّر لعناصرها الحماية من الجرائم الإلكترونيَّة التي تزايدت في السَّنوات الأخيرة نتيجة للطَّفرة الرَّقميَّة التي شَهِدَها العالم.

والأمن هنا لا يَتَوقَّف على الأجهزة الإلكترونيَّة، فهذا جزء من الحماية الواجب توافرها للمُستخدِمين على الإنترنت، لكن أيضًا حماية البيانات والمعلومات المهمَّة، مثل الأمور الماليَّة والأرقام الشَّخصيَّة وكلّ ما من شأنه أن يُمثِّل تهديدًا للفرد أو المؤسَّسة في حال تمّ الكَشْف عنه وإتاحته علنًا، وهذا يشمل البيانات الشَّخصيَّة الموجودة على الهاتف الذَّكيّ، أو على جهاز الحاسوب أو على الأجهزة اللَّوحيَّة، وهنا يقوم دَوْر الأمن السِّيبرانيّ على التَّصدِّي لهذه الهجمات من خلال برامج الدِّفاع الإلكترونيَّة، التي تَمْنع وقوع المشكلة، فيُحافِظ الأمن السِّيبرانيّ على المجتمع وأفراده وبياناته.

ومن أدوات الهجمات الإلكترونيَّة التي تُصيب الأجهزة وتُسَهِّل عمليَّة اختراقها البَرْمَجيَّات الضَّارَّة؛ حيث تهدف إلى الاحتيال والتَّسبُّب في تَلف البيانات وإهدار الأموال، ولا يقتصر الأمر على سرقة البيانات والاحتيال، بل تؤدِّي البَرْمَجيَّات الضَّارَّة أيضًا إلى إتلاف البيانات عن طريق إتلاف كلّ الملفَّات الخاصَّة بالفرد أو المؤسَّسة، وأيضًا إتلاف الأجهزة، الأمر الذي يتسبَّب في كثير من الخسائر المادِّيَّة والمعنويَّة، بسبب تعطيل العمل المبنيّ على هذه الأنظمة والبيانات.

والسَّبب الرَّئيس لتزايد الجرائم الإلكترونيَّة هو اتِّصال أعداد مهولة من الأجهزة على الإنترنت، التي بَلَغَ عددها في عام 2021م نحو 21,1 مليار جهاز، وكان التَّصيُّد الاحتياليّ عن طريق إرسال الرَّوابط الضَّارَّة عبر البريد الإلكترونيّ أبرز هذه الجرائم، وكذلك بَرمَجيَّات الفِدْيَة التي تَمْنع المُستخدِم من الوصول إلى ملفَّاته الموجودة على الجهاز، ويتعيَّن عليه دَفْع الفِدْيَة إلى المُجْرِم حتى يتمكَّن من استرجاع الملفَّات، وغيرها كثير من أشكال التَّهديد والنَّصب وإلحاق الضَّرر بالآخرين.

الفَصْل الأَوَّل

أهمِّيَّة أمن الأجهزة الإلكترونيَّة والشَّبكات

- أوَّلًا: أهمِّيَّة الاستقرار الرَّقميّ للشَّبكات وللأجهزة المتَّصلة بها.
- ثانيًا: المَخاطِر الرَّقميَّة التي تُواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحية).

0 1

أولًا: أهمِّيَّة الاستقرار الرَّقميّ بالنِّسبة للشَّبكات وللأجهزة المتَّصلة بها

تَشْهد البيئة الرَّقميَّة تطوُّرًا متسارعًا، فالاتِّجاه السَّائد في بيئة المعلومات الجديدة هو النُّموّ السَّريع للبيانات الرَّقميَّة وموارد الإنترنت، والتَّوسُّع الدَّائم لشبكة الاتِّصالات العالميَّة؛ حيث تتضمَّن البيئة الرَّقميَّة السِّلسلة الكاملة لتقنيَّات الحاسوب والشَّبكات.

فالمُكوِّن الهيكليّ الأساسيّ للبيئة الرَّقميَّة العالميَّة هو شبكات وأنظمة الاتِّصالات، علمًا بأنَّ الحجم العالميّ للمعلومات يتضاعف كلّ عامين، ووفقًا لشركة Cisco تَجَاوَز حجم حركة مرور IP العالميَّة في عام 2021م تقريبًا 3,3 زيتابايت (الزيتابايت يساوي مليار جيجا بايت)، فمن الممكن الاعتراف بأنّ تقنيَّات الشَّبكات الرَّقميَّة تتشابك بشكلٍ عميقٍ مع نسيج العمليَّات التَّعليميَّة والإنتاجيَّة والتَّمثيليَّة؛ إذ تَستخدِم شبكة الويب العالميَّة أساسًا لإنشاء بيئة رقميَّة مشتركة (بنية تحتيَّة) لرَبْط الآلات والمعدَّات ومَرافِق البنية التَّحتيَّة والنَّقل والسَّلاسل اللُّوجستيَّة والمنظَّمات والمُستخدِمين المقصودين.[1]

وقد أدَّى تَوَسُّع البيئة الرَّقميَّة وظهور وانتشار تقنيَّات الشَّبكات والمعلومات الجديدة إلى النُّموّ العدديّ والنَّوعيّ لمختلف المَخاطِر والتَّهديدات التي يَتَعرَّض لها النَّاس والمجتمعات، وسيؤدِّي هذا بشكلٍ موضوعيّ إلى نموّ أنواع مختلفة من تهديدات سلامة المعلومات، فقد أصبحت تهديدات أمن المعلومات قضيَّة مُلِحَّة بشكلٍ متزايدٍ، ووفقًا لكثير من الخبراء فإنّ إحدى المهامّ الفائقة مُتعدِّدة التَّخصُّصات لهذا القرن هي مُواجَهة التَّهديدات وإدارة المَخاطِر التِّكنولوجيَّة.

إنَّ انتشار تكنولوجيا المعلومات والاتِّصالات، وتوسيع بيئة معلومات الشَّبكة، والجَوْهر التَّفاعليّ الأصليّ للإنترنت، وظهور الشَّبكات الاجتماعيَّة، يؤدِّي إلى مخاطر وتهديدات جديدة لأمن المعلومات، ويؤدِّي بشكلٍ غير مُباشِرٍ إلى زعزعة الاستقرار الاجتماعيّ؛ فالاستخدام واسع النِّطاق لتقنيَّات الشَّبكات الحديثة يخلق متطلَّبات مسبقة محتملة لمثل هذه التَّهديدات، مثل تَسَرُّب المعلومات والسَّرقة والتَّشويه والنَّسْخ والانتحال والحَجْب، وبالتَّالي الأضرار الاقتصاديَّة والبيئيَّة والاجتماعيَّة وغيرها من أنواع الأضرار.

1. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97-106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088.

ومـن خـلال اختراقاتهـم غيـر المُصـرَّح بهـا لشـبكات الحاسـوب، لا يَنْسـخ المجرمـون المعلومـات المُخزَّنـة هنـاك فحسـب، بـل يُلَوِّثونهـا بِبَرمَجيَّـات ضَـارَّة تُدَمِّـر الأجهـزة وتُتْلِـف بعـض محتوياتهـا.

وبحسـب شـركة Positive Technologies فـإنّ إحصائيَّـات التَّهديـدات السِّـيبرانيَّة فـي عـام 2018م كانـت علـى النَّحـو التَّالـي: بلغـت حصـص الهجمـات المقصـودة، والهجمـات التـي تهـدف إلـى سـرقة البيانـات الشَّخصيَّة والمحاسـبيَّة وبيانـات بطاقـات الدَّفْـع 62 و30 و24 و14% علـى التَّوالـي؛ وتـمّ اسـتخدام البَرمَجيَّـات الضَّـارَّة فـي 56% مـن الهجمـات الإلكترونيَّـة.[1]

كمـا أنّ وجـود إنترنـت الأشـياء ألقـى بظلالـه علـى المَخاطِـر السِّـيبرانيَّة علـى الأفـراد، فوفقًـا للدِّراسـات التـي أجراهـا معهـد ماساتشوسـتس للتِّكنولوجيـا، فـإنّ حـالات الانقطـاع والفشـل المتتاليـة بسـبب أخطـاء البَرمَجيَّـات والعيـوب ستصبح جـزءًا مـن روتيننـا اليومـيّ وتَصِـل إلـى العشـرات والمئـات مـن الحـالات كلّ عـام، وبالتَّالـي فـإنّ المَخاطِـر الاقتصاديَّـة والاجتماعيَّـة الرَّئيسـة المحتملـة لإنترنـت الأشـياء لا تكمـن فـي اسـتغلال المُتسـلِّلين لهـا، بـل فـي وجودهـا ذاتـه ومواصلـة تطويرهـا.

أمن المعلومات Information Security

يُقصَـد بـه الوسـائل والأدوات والإجـراءات الـلَّازم توفيرهـا لضمـان حمايـة المعلومـات مـن الأخطـار الدَّاخليَّـة والخارجيَّـة، وهـو العِلْـم الـذي يَـدْرُس كيفيَّـة توفيـر تدابيـر حمايـة سـرِّيَّة وسـالمة للمعلومـات وكيفيَّـة مُكَافَحَـة الاعتـداء عليهـا.

وتقـوم حمايـة المعلومـات علـى عـدَّة خطـوات تضمـن حمايـة الأجهـزة والشَّـبكات مـن الاختـراق، وهـي:

- استخدام كلمات مرور قويَّة، وتغييّرها من حين إلى آخر.
- حماية الحاسوب من المُتسلِّلين عبر برامج مُكَافَحَة الفيروسات.
- حماية البرامج والبيانات عبر النسخ الاحتياطيّ.
- استخدام جدار الحماية Firewall.[2]

1. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088

2. إبراهيم، حمادي عثمان. أمن المعلومات، محاضرات مادّة الحاسوب، قسم اللُّغة الإنجليزيَّة، كلّيَّة التَّربية للعلوم الإنسانيَّة، جامعة الأنبار، العراق. متاح على الرَّابط: https://www.uoanbar.edu.iq/eStoreImages/Bank/1352.pdf.

أمن الشبكات Network Security

هو جزء من منظومة أمن المعلومات التي تقوم على حماية استخدام الشَّبكة وسلامتها ومن ثمّ سلامة عمليّات نقل وتبادل البيانات، ويشمل هذا المجال كلًّا من تكنولوجيا الأجهزة والبرامج، ويُدير أمن الشَّبكات الفعّال إمكانيّة الوصول إلى الشَّبكة، ويَستهدِف مجموعةً مُتنوِّعةً من التَّهديدات ويَمْنَعُها من الدُّخول إلى شبكتك أو من الانتشار.

ويَجْمع أمن الشَّبكات بين طبقات مُتعدِّدة من الدِّفاعات؛ حيث تقوم كلّ طبقة من أمن الشَّبكات بتنفيذ السِّياسات وعناصر التَّحكُّم، وبناءً على ذلك يمكن للمُستخدِمين المُصرَّح لهم الوصول إلى موارد الشَّبكة، لكن يتمّ مَنْع الجهات الفاعلة الخبيثة من تنفيذ عمليّات الاستغلال والتَّهديدات.

وتقوم برامج أمن الشَّبكات على عدَّة أساسيَّات، فيما يلي تبيان لأهمِّها

1. التَّحكُّم في الوصول

يُقصَد به فَرْض سياسات أمان تَمْنَع المُستخدِمين غير المُصرَّح لهم باستخدام شبكتك من الدُّخول إليها ومن ثمّ من الوصول إلى أجهزتك وبياناتك؛ حيث يمكن للمُستخدِم مالِك الشَّبكة حَظْر أجهزة نقطة النِّهاية غير المتوافقة أو مَنْحها وصولًا محدودًا فقط، ويُطْلَق على هذه العمليَّة "التَّحكُّم في الوصول إلى الشَّبكة" network access control.

2. برامج مُكَافَحَة الفيروسات والبرمجيَّات الخبيثة

تتضمَّن البرمجيَّات الخبيثة Malware وهي اختصار لـ (malicious software) وتشمل ديدان الحاسوب وأحصنة طروادة وبَرْمَجيَّات الفِدْيَة وبَرْمَجيَّات التَّجسُّس؛ وتُصيب البرمجيَّات الخبيثة الشَّبكة أحيانًا، ولكنَّها تظلّ كامنة -أي نائمة- لمدَّة أيَّام أو حتى أسابيع، وهنا تأتي أهمِّيَّة برامج مكافحة البرمجيَّات الضَّارة.

أمان التَّطبيقات

يشمل أمان التَّطبيق الأجهزة والبرامج والعمليَّات التي تستخدمها لإغلاق الثَّغرات الموجودة في التَّطبيقات.

4. التَّحليل السُّلوكيّ

تقوم أدوات التَّحليل السُّلوكيّ بالتَّمييز التِّلقائيّ للأنشطة التي يُشْتَبه بها لمعالجتها سريعًا.

5. حماية البيانات

تَمْنع تقنيَّات مَنْع فقدان البيانات أو DLP الأشخاص من تحميل أو إعادة توجيه أو حتى طباعة المعلومات المهمَّة بطريقة غير آمِنة.

6. أمان البريد الإلكترونيّ

يُعَدّ البريد الإلكترونيّ أحد أهمّ المنافذ التي يتسلَّل من خلالها المُهاجِمون إلى الأجهزة؛ بهدف طَلَب الفِدْيَة والابتزاز والتَّصيُّد الاحتياليّ، لذا يحظر تطبيق أمان البريد الإلكترونيّ الهجمات الواردة ويتحكَّم في الرَّسائل الصَّادرة لمَنْع فقدان البيانات الحسَّاسة.

7. جدران الحماية

تعمل جدران الحماية على وَضْع حاجز بين شبكتك الدَّاخليَّة الموثوقة والشَّبكات الخارجيَّة غير الموثوق بها، مثل الإنترنت؛ حيث تَستخدِم مجموعة من القواعد المُحدَّدة للسَّماح بالزِّيارات أو مَنْعها.

8. أنظمة مَنْع التَّجسُّس

يقوم نظام مَنْع التَّجسُّس (IPS) بفَحْص حركة مرور البيانات عبر الشَّبكة؛ لمَنْع الهجمات بشكلٍ فعَّالٍ.

9. أمان الجهاز المحمول

يَستهدِف مُجْرمو الإنترنت بشكلٍ متزايدٍ الأجهزة المحمولة والتَّطبيقات، لذا تتزايد الحاجة إلى التَّحكُّم في الأجهزة التي يمكنها الوصول إلى شبكتك.

10. تقنيَّات تقسيم وعَزْل الشَّبكة

تَضَع البرامج المعرفة بالتَّقسيم زيارات الشَّبكة ضمن تصنيفات مختلفة؛ حيث يمكن لمالِك الشَّبكة مَنْح المستوى المناسب للوصول إلى الأشخاص المناسبين وتضمين الأجهزة المشبوهة ومعالجتها.

11. أمن الويب

يَعْمَل أمن الويب على مَنْع تهديدات الويب ومَنْع الوصول إلى مواقع الويب الضَّارَّة.[1]

1. What Is Network Security? cisco. On site: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

ثانيًا: المَخاطِر الرَّقميَّة التي تواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحيَّة)

تواجه الأجهزة الرَّقميَّة جملة من التَّحدِّيات والمَخاطِر، فيما يلي تبيان لأهمِّها

1. تَسَرُّب البيانات

في بعض الأحيان تكون تطبيقات الأجهزة المحمولة سببًا في تَسَرُّب البيانات غير المُتعمَّد. فعلى سبيل المثال، تُشكِّل تطبيقات "البَرمَجيَّات الخطرة"، التي تأتي كتطبيقات مجانيَّة، مشكلةً حقيقيَّةً لمُستخدِمي الأجهزة المحمولة، الذين يمنحونها أذونات شاملة ولكن لا يتحقَّقون من الأمن دائمًا؛ حيث تُرْسِل البيانات الشَّخصيَّة وربَّما بيانات العمل إلى خادم بعيد، ما يُتيح الفرصة للمُجْرمين الإلكترونيِّين لاستغلالها، ولتَجَنُّب هذه المشكلة لا تَمْنح التَّطبيقات إلَّا الأذونات الضَّروريَّة للغاية وتَجَاهَلْ أيّ برنامج يَطْلُب أكثر من اللَّازم.[1]

2. تزوير الشَّبكة

عادةً ما تكون شبكات Wi-Fi المجانيَّة أو (العامَّة) غير آمِنة، ولكي يكون المُستخدِم بمأمن من الهجمات الإلكترونيَّة، عليه ألَّا يَستخدِم شبكة Wi-Fi المجانيَّة على جهازه المحمول إلا نادرًا، ولا يَستخدِمها مطلقًا للوصول إلى الخدمات السِّرِّيَّة أو الشَّخصيَّة، مثل المعلومات المصرفيَّة أو معلومات بطاقات الائتمان.

ويحدث تزوير الشَّبكة عندما يقوم المُتسلِّلون بإعداد نقاط اتِّصال مزيَّفة تبدو مثل شبكات Wi-Fi عامَّة ولكنَّها في الواقع مجرَّد فخّ، مثل الموجودة في المقاهي والمكتبات والمطارات؛ حيث يُسمِّي المُجْرمون الإلكترونيُّون نقاط الاتِّصال بأسماء عامَّة، مثل "شبكة Wi-Fi مجانيَّة للمطار" أو "المقهى"؛ لكي تُشَجِّع المُستخدِمين على الاتِّصال بها.

وقد يُطالِب المُهاجِم المُستخدِمين بإنشاء "حساب" للوصول إلى هذه الخدمات المجانيَّة، ويكتمل الأمر بطلب كلمة المرور، ولأنّ جزءًا كبيرًا يلجأ إلى تكرار نفس كلمة المرور والبريد الإلكترونيّ في الدُّخول إلى عدَّة حسابات يصبح بإمكان هؤلاء المُتسلِّلين الوصول إلى كافَّة البيانات الخاصَّة[2]؛ لذا يُفضَّل تَوَخِّي الحَذَر عند الاتِّصال بأيّ شبكة Wi-Fi عامَّة، وإذا طُلِبَ منك إنشاء تسجيل دخول، فاخْتَر إدخال كلمة مرور مختلفة دائمًا.

1. Mobile Cyber Threats, Kaspersky Lab&Interpol Joint Report. On site: https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf.
2. موصلي، طارق. 7 تهديدات أمنيَّة عند استخدام شبكة الواي فاي العامَّة (وكيف تحمي نفسك منها)، أمن المعلومات، 2021م، متاح على الرَّابط: https://cutt.us/cb7w0.

3. هجمات التَّصيُّد الاحتياليّ

تُمثِّل الأجهزة المحمولة الخطوط الأماميَّة لهجمات التَّصيُّد الاحتياليّ، نظرًا لكونها مشغَّلة بشكلٍ دائمٍ، لذا يُعَدّ مُستخدِمو الأجهزة المحمولة الأكثر عُرْضةً للهجمات؛ لأنَّهم غالبًا ما يكونون أوَّل مستلمي رسائل البريد الإلكترونيّ التي تبدو شرعيَّة ويلتقطون الطُّعم، لذا يجب عدم النَّقْر مطلقًا فوق روابط البريد الإلكترونيّ غير المألوفة التي يكون التَّحقُّق منها أصعب على شاشات أجهزة المحمول الصَّغيرة، وهنا يُفضَّل إدخال عناوين URL يدويًّا كي تكون آمِنةً قَدْر الإمكان.

4. بَرْمَجيَّات التَّجسُّس

لحماية الأجهزة من بَرْمَجيَّات التَّجسُّس يجب تنزيل مجموعة برامج فعَّالة لمُكَافَحَة الفيروسات وكَشْف البَرْمَجيَّات الضَّارَّة والتَّخلُّص منها قبل أن تُتاح لها فرصة جَمْع بياناتك الشَّخصيَّة.

5. التَّشفير المعطّل

يمكن أن يحدث تَعَطُّل في التَّشفير عندما يَستخدِم مُطوِّرو التَّطبيقات خوارزميَّات تشفير ضعيفة أو تشفيرًا قويًّا من دون عمليَّة تطبيق سليمة، وفي الحالة الأولى، يَستخدِم المُطوِّرون خوارزميَّات تشفير تحتوي على ثغرات أمنيَّة معروفة بالفعل لتسريع عمليَّة تطوير التَّطبيق، والنتيجة أنَّه يمكن للمُهاجِمين اختراق كلمات المرور والوصول إلى ما يريدون على الأجهزة. أمَّا في المثال الثَّاني، فيَستخدِم المُطوِّرون خوارزميَّات آمِنة للغاية، ولكنَّهم يتركون "مداخل سرِّيَّة" أخرى تحدّ من فعاليَّتها، فمثلًا: قد لا يتمكَّن المُهاجِمون من اختراق كلمات المرور، لكن إذا ترك المُطوِّرون أخطاءً برمجيَّة تَسْمح للمُهاجِمين بتعديل وظائف التَّطبيقات عالية المستوى كإرسال الرَّسائل النَّصِّيَّة أو تلقِّيها، حينها لا يحتاجون إلى كلمات مرور لإحداث مشكلات للمُستخدِمين.[1]

وعمومًا تَشْهَد تهديدات أمن الأجهزة المحمولة تغيُّرًا كبيرًا، وهناك ثلاثة مجالات أساسيَّة أكثر تأثُّرًا وهي:

- الحواسيب: تُعدّ الحواسيب عُرْضَةً لتهديدات الاختراق بشكلٍ كبيرٍ، كما أنَّها تُعدّ مَدْخلاً لاختراق الهواتف الذَّكيَّة والأجهزة اللَّوحيَّة، فعَدْوَى الاختراق قد تنتقل من الحواسيب إلى الأجهزة الأخرى المُتَّصلة بها.
- الهواتف الذَّكيَّة والأجهزة اللَّوحيَّة: تُواجِه الهواتف الذَّكيَّة والأجهزة اللَّوحيَّة تهديدات بالاختراق تَفُوق التَّهديدات التي تَتعرَّض لها الحواسيب؛ وذلك نظرًا لكون برامج الحماية المُصمَّمة للهواتف الذَّكيَّة وللأجهزة اللَّوحيَّة تُعدّ أقلّ تطورًا وكفاءة من تلك المُصمَّمة للحواسيب.
- اتِّساع نطاق الأجهزة الذَّكيَّة: في ظلّ التَّطوُّر التكنولوجيّ المُتسارِع، ازداد انتشار الأجهزة الذَّكيَّة في المنازل وفي بيئة الأعمال، لا سيَّما الأجهزة المُرتبِطَة بالمنازل الذَّكيَّة، وهذا التَّعدُّد في الأجهزة الذَّكيَّة يزيد من فُرَص التَّعرُّض للاختراق؛ خاصَّةً أنَّ هذه الأجهزة غالبًا ما تكون مُتَّصِلَة ببعضها، فاختراق أحدها يعني انتقال الاختراق لباقي الأجهزة[2]

1. Broken cryptography, resources. On site: https://cutt.us/an1BC.
2. Top Trends and Threats in Mobile Security: Gartner, cxotoday. On site: https://cutt.us/oMMsw.

الفَصْل الثَّاني

أنواع المَخاطِر الرَّقميَّة التي تُواجه الأجهزة

- أوَّلًا: هجوم الفِدْيَة.
- ثانيًا: سرقة بيانات الأجهزة.
- ثالثًا: الوصول غير القانونيّ.
- رابعًا: البرمجيَّات الضَّارَّة.

02

أولًا: هجوم الفِدْيَة

هناك العشرات من أنواع بَرمَجيَّات الفِدْيَة لكلّ منها خصائصه، نذكر منها:

1. ريوك Ryuk

يعمل هذا البرنامج من الفِدْيَة عبر رسائل البريد الإلكترونيّ للتَّصيُّد الاحتياليّ أو باستخدام بيانات اعتماد المُستخدِم المُخترقَة لتسجيل الدُّخول إلى أنظمته أو أنظمة المؤسَّسة العامل بها، وبمجرَّد إصابة النِّظام يقوم Ryuk بتشفير أنواع معيَّنة من الملفَّات ثمّ يُقدِّم طَلَب فِدْيَة، وهو من أكثر بَرمَجيَّات الفِدْيَة ضررًا، فهو يَطْلُب فِدْيَة يزيد متوسِّطها على مليون دولار.

2. المتاهة Maze

يشتهر برنامج الفِدْيَة هذا بكونه أوَّل برنامج يَجْمَع بين تشفير الملفَّات وسرقة البيانات، فهو يعمل على جَمْع البيانات الحسَّاسة من أجهزة الحاسوب الخاصَّة بالضَّحايا قبل تَشْفيرها، وإذا لم يتمّ تلبية طلبات الفِدْيَة يَكْشِف عن هذه البيانات علنًا أو يَبيعها لمَن يَدْفع أعلى سعر.

3. REvil / Sodinokibi

هو أحد أشكال بَرمَجيَّات الفِدْيَة الأخرى التي تَستهدِف المؤسَّسات الكبيرة؛ حيث يَستخدِم مُجْرمو الإنترنت تقنيَّة الابتزاز المزدوج لسرقة البيانات من الشَّركات مع تشفير الملفَّات أيضًا، ما يعني أنَّه إلى جانب المُطالَبة بفِدْيَة لفكّ تشفير البيانات، فإنَّهم يُهدِّدون بالإفراج عن البيانات المسروقة إذا لم يتمّ سداد دفعة ثانية.

4. قفل LockBit

هو برنامج ضار يستهدف المؤسسات الكبيرة، بدأ البرنامج هجماته منذ عام 2018م، وخطورة هذا البرنامج تتمثل في صعوبة اكتشافه من قِبَل برامج مكافحة الفيروسات.

5. عزيزي كراي

في مارس 2021م، أَصْدَرت Microsoft تصحيحات لأربع ثغرات أمنيَّة داخل خوادم Microsoft، وهذا البرنامج من الفِدْيَة صُمِّم للاستفادة من أربع ثغرات أمنيَّة تمّ الكَشْف عنها مؤخَّرًا في Microsoft Exchange؛ حيث يعمل على تشفير أنواع معيَّنة من الملفَّات، ثمّ إرسال رسالة فِدْيَة تَطْلُب من المُستخدِمين إرسال بريد إلكترونيّ إلى مُشَغِّلي بَرمَجيَّات الفِدْيَة لمعرفة كيفيَّة فكّ تشفير ملفَّاتهم.

6. لابسوس Lapsus

هي عصابة من بَرمَجيَّات الفِدْيَة في أمريكا الجنوبيَّة تمّ رَبْطها بهجمات إلكترونيَّة على بعض الأهداف البارزة، وتشتهر بالابتزاز؛ حيث تُهدِّد بنَشْر معلومات حسَّاسة، وسَبَقَ لها اختراق سامسونج Samsung، فهي تُخْفي ملفَّات البَرمَجيَّات الضَّارَّة على أنَّها ملفَّات جديرة بالثِّقة.[1]

1. What is Ransomware? checkpoint. On Site: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

كيفيَّة عمل بَرمَجيَّات الفِدْيَة

لنجاح بَرمَجيَّات الفِدْيَة في تحقيق أهدافها الخبيثة تحتاج إلى الوصول إلى النِّظام المُستهدَف وتشفير الملفَّات عليه ثمّ طَلَب فِدْيَة من الضَّحيَّة، **وهناك ثلاث مراحل أساسيَّة تَمُرّ بها هذه العمليَّة:**

1. ناقلات العدوى والتَّوزيع

مثل أيّ برنامج ضارّ، هناك عدَّة طُرُق للوصول إلى أنظمة المُستخدِم الضَّحيَّة المُستهدَف، سواءٌ أكان فردًا أم مؤسَّسةً، لكن يميل مُشَغِّلو بَرمَجيَّات الفِدْيَة إلى استخدام عدد قليل من نواقل العدوى المُحدَّدة، أي قنوات الإصابة، وإحدى هذه القنوات المُفضَّلة لهم هي رسائل البريد الإلكترونيّ التَّصيُّديَّة ومواقع الإنترنت المَشبوهَة.

وقد تحتوي رسالة البريد الإلكترونيّ الضَّارَّة على رابط إلى موقع ويب يستضيف تنزيلًا ضارًّا أو مُرْفَقًا يحتوي على وظيفة التَّنزيل المُضمَّنة، بحيث إذا وَقَعَ مُستلِم البريد الإلكترونيّ في فخّ التَّصيُّد الاحتياليّ يتمّ تنزيل برنامج الفِدْيَة وتنفيذه على جهاز الحاسوب الخاصّ به.

2. تشفير البيانات

بمجرَّد أن يتمكَّن مُجْرمو الإنترنت من الوصول إلى نظام الحاسوب سواءٌ للفرد أم للمؤسَّسة، يبدأ تشفير ملفَّاته باستخدام مفتاح يَتَحكَّم فيه المُهاجِم، واستبدال النُّسَخ الأصليَّة بالإصدارات المُشفَّرة، وغالبًا يتمّ اختيار هذه الملفَّات بِحَذَر لضمان استقرار النِّظام؛ لأنّ الهدف هنا هو المال وليس التَّدمير المُطْلَق للنِّظام.

3. طلب الفِدْيَة

بعد اكتمال تشفير الملفّ، يصبح برنامج الفِدْيَة جاهزًا لتقديم طَلَب فِدْيَة، وتُنَفِّذ المُتغيِّرات المختلفة لبَرمَجيَّات الفِدْيَة هذا بطُرُق عدَّة، وعادةً ما يَطْلُب مبلغًا مُحدَّدًا من العملة المُشفَّرة مقابل الوصول إلى ملفَّات الضَّحيَّة؛ وإذا تمّ دَفْع الفِدْيَة، يقوم مُشَغِّل برنامج الفِدْيَة بتسهيل وصول الضَّحيَّة إلى ملفَّاته لاستخدامها مجدَّدًا.[1]

1. How Ransomware Works, unitrends. On Site: https://www.unitrends.com/solutions/ransomware-education.

كيفيَّة الحماية من بَرمَجيَّات الفِدْيَة

يساعد الإعداد المُناسِب إلى تقليل تكلفة وتأثير هجوم بَرمَجيَّات الفِدْيَة بشكلٍ كبيرٍ، ويمكن أن يؤدّي اتّباع أفضل الممارسات التّالية إلى تقليل تَعَرُّض الأفراد والمؤسَّسات لبَرمَجيَّات الفِدْيَة وتقليل آثارها، **وفيما يلي تبيان لأهمّ الإجراءات التي من الممكن أن تُقلِّل من خطر التَّعَرُّض لهجوم الفِدْيَة.**

- **التَّعليم والتَّأهيل والتَّدريب على مفاهيم السَّلامة الرَّقميَّة والأمن السّيبرانيّ**

غالبًا ما تنتشر بَرمَجيَّات الفِدْيَة باستخدام رسائل البريد الإلكترونيّ التَّصيُّديَّة ومواقع الإنترنت المَشبوهَة؛ لذا يُفضَّل التَّدريب على كيفيَّة التَّعرُّف على هجمات بَرمَجيَّات الفِدْيَة المحتملة وتَجَنُّبها.

- **النَّسْخ الاحتياطيّ المستمرّ للبيانات**

بَرمَجيَّات الفِدْيَة هي بَرمَجيَّات ضارَّة مُصمَّمة لجَعْل دَفْع الفِدْيَة هو الطَّريقة الوحيدة لاستعادة الوصول إلى البيانات المُشفَّرة، لذا النَّسَخ الاحتياطيَّة التِّلقائيَّة للبيانات تُساعِد المُستخدِمين على التَّعافي من الهجوم مع الحدّ الأدنى من فقدان البيانات ودون دَفْع فِدْيَة.

- **التَّحديث والتَّصحيح**

يُعَدّ التَّصحيح عنصرًا حاسمًا في الدِّفاع ضدّ هجمات بَرمَجيَّات الفِدْيَة؛ حيث يبحث مُجْرمو الإنترنت غالبًا عن الثَّغرات في الأنظمة التي لم تُصحَّح بعدُ، لذا من المهمّ أن يتأكَّد المُستخدِم أنّ جميع الأنظمة لديها أَحْدَث التَّصحيحات المُطبَّقة عليها، فهذا يُقلِّل من عدد نقاط الضَّعف المحتملة التي يمكن للمُهاجِم استغلالها، والتَّحديث يرتبط بالتَّحديث المُستمِرّ لبرامج مُكافَحَة البَرْمَجيَّات الضَّارَّة.

- **مصادقة المُستخدِم**

يُعَدّ الوصول إلى بعض الخدمات باستخدام بيانات اعتماد المُستخدِم المسروقة أسلوبًا مُفضَّلًا لمُهاجِمي بَرمَجيَّات الفِدْيَة، لذا يُعَدّ استخدام مصادقة المُستخدِم القويَّة وسيلةً مهمَّةً لمَنْع المُهاجِم من الاستفادة من كلمة المرور التي تمّ تخمينها أو سَرقتها.

- **تقليل سَطْح الهجوم**

إنّ الوقاية هي أفضل إستراتيجيَّة للتَّخفيف من آثار بَرمَجيَّات الفِدْيَة، ويمكن تحقيق ذلك بتقليل سَطْح الهجوم عن طريق معالَجة:

- رسائل التَّصيُّد.
- نقاط الضَّعف غير المُصحَّحة.
- حلول الوصول عن بُعْد.
- البَرمَجيَّات الضَّارَّة للهواتِف الذَّكيَّة.[1]

1. What do I do to protect against Ransomware? security.berkeley.edu. On Site: https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware.

كيفيَّة التَّخفيف من عدوى بَرمَجيَّات الفِدْيَة النَّشطة

يتمّ اكتشاف كثير من هجمات بَرمَجيَّات الفِدْيَة النَّاجحة بعد اكتمال تشفير البيانات وعَرْض مُذَكِّرة فِدْيَة على شاشة الحاسوب المصاب، وفي هذه المرحلة تكون الملفَّات المُشفَّرة غير قابلة للاسترداد، **لكن يجب اتِّخاذ بعض الخطوات على الفور:**

- **عَزْل الجهاز:** تعمل بعض أنواع بَرمَجيَّات الفِدْيَة على الانتشار في مُحرِّكات الأقراص المتَّصلة والأجهزة الأخرى، لذا يجب قَطْع الطَّريق أمامها عبر عَزْل الجهاز الذي تَلَقَّى رسالة الفِدْيَة عن باقي الأجهزة المتَّصلة به.
- **اتْرُك الحاسوب قَيْد التَّشغيل:** يؤدِّي تشفير الملفَّات إلى جَعْل الحاسوب غير مستقرّ، لذا فإنّ إيقاف تشغيل الحاسوب ليس الحلّ الأكيد؛ لأنَّه قد يؤدِّي إلى فقدان الذَّاكرة.
- **إنشاء نسخة احتياطيَّة:** قُمْ بعمل نسخة من الملفَّات المُشفَّرة على الوسائط القابلة للإزالة.
- **التَّحقُّق من وجود أدوات فكّ التَّشفير:** تَحَقَّق من مشروع No More Ransom Project لمعرفة ما إذا كان برنامج فكّ التَّشفير المجانيّ متاحًا أم لا، وإذا كان الأمر كذلك، قُمْ بتشغيله على نسخة من البيانات المُشفَّرة لمعرفة ما إذا كان يمكنه استعادة الملفَّات.
- **اطْلُب المساعدة:** تقوم أجهزة الحاسوب أحيانًا بتخزين نُسَخ احتياطيَّة من الملفَّات المُخزَّنة عليها، ويمكن أن يساعد شخص مُتخصِّص في استعادة هذه النُّسَخ إذا لم يتمّ حَذْفها بواسطة البَرمَجيَّات الضَّارَّة.
- **المَسْح والاستعادة:** استعادة الجهاز من نسخة احتياطيَّة نظيفة أو تثبيت نظام التَّشغيل، لضمان إزالة البَرمَجيَّات الضَّارَّة بالكامل من الجهاز.[1]

1. Mitigating malware and ransomware attacks, how to defend organisations against malware or ransomware attacks. On Site: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

ثانيًا: سرقة بيانات الأجهزة

تعريف سرقة البيانات

سرقة البيانات -المعروفة أيضًا بسرقة المعلومات- هي نَقْل أو تَخْزين غير قانونيّ للمعلومات الشَّخصيَّة أو السِّرِّيَّة أو الماليَّة، ويمكن أن يشمل ذلك كلمات المرور أو التَّعليمات البرمجيَّة أو الخوارزميَّات البرمجيَّة والعمليَّات أو التِّقنيَّات الخاصَّة، وتُمثِّل انتهاكًا خطيرًا للأمان والخصوصيَّة.

إذًا هي عمليَّة سرقة المعلومات الرَّقميَّة المَخزَّنة على أجهزة الحاسوب أو الخوادم أو الأجهزة الإلكترونيَّة للحصول على معلومات سرِّيَّة أو المساس بالخصوصيَّة، وبمجرَّد وصول شخص غير مُصرَّح له إلى تلك المعلومات يمكنه حَذْفها أو تغييرها أو مَنْع الوصول إليها دون إذْن المالِك.

وتحدث سرقة البيانات عادةً لأنّ الجِهات الفاعلة الخبيثة ترغب في بَيْع المعلومات أو استخدامها لسرقة الهُوِيَّة، ولا تعني سرقة حرفيًّا أَخْذ المعلومات أو إزالتها من الضَّحيَّة، لكن يقوم المُهاجِم ببساطة بنَسْخ المعلومات أو تكرارها لاستخدامه الخاصّ.

ويُطْلَق على سرقة البيانات أيضًا المُصْطَلحان "خَرْق البيانات" و"تَسَرُّب البيانات" لكن هناك فروقًا بسيطة بين هذه المفاهيم، هي:

- يحدث تَسَرُّب البيانات عندما يتمّ الكَشْف عن بيانات حسَّاسة عن طريق الخطأ، إمَّا على الإنترنت وإمَّا من خلال مُحرِّكات الأقراص الثَّابتة أو الأجهزة المفقودة، أي يمكن لمُجْرمي الإنترنت الوصول غير المُصرَّح به إلى البيانات الحسَّاسة دون جهدٍ منهم.
- يُشير خَرْق البيانات إلى الهجمات الإلكترونيَّة المُتعمَّدة.[1]

1. العكايلة، عبد الله ماجد عبد المطّلب. سرقة البيانات والمعلومات الإلكترونيَّة "دراسة مقارنة"، كلّيَّة العلوم والدِّراسات الإنسانيَّة - قسم القانون، جامعة الأمير سطام بن عبد العزيز. متاح على الرَّابط: https://jfslt.journals.ekb.eg/article_10943_869bcc9f604774fe726ffe0bc9e5878b.pdf.

كيف تحدث سرقة البيانات؟

تحدث من خلال مجموعة مُتنوِّعة من الأدوات، فيما يلي تبيان لأهمِّها:

1. الهندسة الاجتماعيَّة

الشَّكل الأكثر شيوعًا للهندسة الاجتماعيَّة هو التَّصيُّد الاحتيالي، ويحدث عندما يَتَنَكَّر المُهاجِم في صورة كيان موثوق به؛ لخِداع الضَّحيَّة لفَتْح بريد إلكتروني أو رسالة نصِّيَّة أو رسالة فوريَّة.

2. كلمات المرور الضَّعيفة

إنّ استخدام كلمة مرور يَسْهُل تخمينها أو استخدام نفس كلمة المرور لحسابات مُتعدِّدة، يمكن أن يَسْمَح للمُهاجِمين بالوصول إلى البيانات، كما يمكن أن تؤدي عادات كلمة المرور السَّيِّئة مثل كتابة كلمات المرور على قطعة من الورق أو مشاركتها مع الآخرين إلى سرقة البيانات.

3. نقاط ضعف النِّظام

التي تمّ تصميمها أو تنفيذها بشكلٍ سيِّئٍ إلى إنشاء ثغرات أمنيَّة يمكن للمُتسلِّلين استغلالها واستخدامها لسرقة البيانات، كما تؤدِّي برامج مُكَافَحَة الفيروسات القديمة أيضًا إلى إنشاء ثغرات أمنيَّة.

4. التَّهديدات الدَّاخليَّة

يمكن للمُوظَّفين الذين يعملون في مؤسَّسةٍ ما الوصول إلى المعلومات الشَّخصيَّة للعملاء واستغلالها.

5. الخطأ البشريّ

في بعض الأحيان يمكن أن تكون سرقة البيانات نتيجة خطأ بشريّ، مثل إرسال معلومات حسَّاسة إلى الشَّخص الخطأ، أو إرسال بريد إلكترونيّ عن طريق الخطأ إلى عنوان غير صحيح، أو إرفاق مُسْتَنَد خاطئ، أو تسليم ملفٍّ فعليٍّ إلى شخص لا ينبغي له الوصول إلى المعلومات.

6. تثبيت برامج من مصادر غير موثوقة

قد يقوم أحد الأشخاص بتنزيل برامج أو بيانات من مواقع الويب المُخترَقة والمصابة بفيروسات، مثل الفيروسات المُتنقِّلة أو البَرمَجيَّات الضَّارَّة.

7. فقدان الأجهزة الإلكترونيَّة

بعض عمليَّات سرقة البيانات ليست نتيجةً لجريمة إلكترونيَّة، مثل سرقة أو ضياع ملفَّات إلكترونيَّة أو ورقيَّة، أو سرقة أو ضياع الأجهزة الإلكترونيَّة، ومع تزايد انتشار العمل عن بُعْد، زاد أيضًا احتمال فقدان الأجهزة أو سرقتها، وإذا كنت تعمل في مكان عامٍّ مثل المقهى، فقد يتمكَّن شخص ما من مراقبة شاشتك ولوحة المفاتيح لسرقة معلومات مثل تفاصيل تسجيل الدُّخول الخاصَّة بك.

8. المعلومات المتاحة للجمهور

يمكن العثور على كثير من المعلومات من خلال عمليَّات البحث على الإنترنت والبحث في منشورات المُستخدِمين على الشَّبكات الاجتماعيَّة.[1]

1. What is data theft and how to prevent it, Kaspersky. On Site: https://www.kaspersky.com/resource-center/threats/data-theft.

ما أنواع البيانات التي تتمّ سرقتها؟

1. سجلّات العملاء.
2. البيانات الماليّة، مثل معلومات بطاقة الائتمان أو بطاقة الخَصْم.
3. رموز المصدر والخوارزميّات.
4. أوصاف عمليّة المِلْكِيّة ومنهجيّات التّشغيل.
5. بيانات اعتماد الشّبكة، مثل أسماء المُستخدِمين وكلمات المرور.
6. سجلّات الموارد البشريّة وبيانات المُوظّفين.
7. المستندات الخاصّة المُخزّنة على أجهزة الحاسوب.[1]

عواقب سرقة البيانات

من الممكن أن يواجه الأشخاص الذي يقومون بسرقة البيانات ما يلي:

1. الدّعاوى القضائيّة المحتملة من العملاء الذين تمّ الكَشْف عن معلوماتهم.
2. طَلَبات الفِدْيَة من المُهاجِمين.
3. تكاليف الاسترداد، على سبيل المثال، استعادة أو تصحيح الأنظمة التي تمّ اختراقها.
4. الإضرار بالسُّمعة وخسارة العملاء.
5. الغرامات أو العقوبات من الهيئات التّنظيميّة حسب الصّناعة.
6. التّوقُّف في أثناء استعادة البيانات.
7. بالنّسبة للأفراد الذين تمّ اختراق بياناتهم، فإنّ النّتيجة الرّئيسة هي أنّ ذلك قد يؤدّي إلى سرقة الهُوِيّة، ما يُسبِّب خسارةً ماليّةً واضطرابًا عاطفيًّا.

1. The 5 most common types of data stolen, Lewis Morgan, March 2014. On Site: https://www.itgovernance.co.uk/blog/the-5-most-common-types-of-data-stolen.

كيفيَّة الحفاظ على البيانات آمِنة

يمكن المحافظة على أمن البيانات من خلال اتِّباع ما يلي:

1. اسْتخدِم كلمات مرور آمِنة قويَّة وتغييرها من حين إلى آخر

يمكن للمُتسلِّلين اختراق كلمات المرور بسهولة إذا كنت لا تَستخدِم كلمة مرور قويَّة، لذا يجب أن تتكوَّن كلمة المرور القويَّة من 12 حرفًا على الأقلّ أو أكثر، وتتكوَّن من مزيج من الأحرف الكبيرة والصَّغيرة، بالإضافة إلى الرُّموز والأرقام.

2. تَجَنَّب استخدام نفس كلمة المرور لحسابات مُتعدِّدة

إذا كنت تَستخدِم نفس كلمة المرور لحسابات مُتعدِّدة، فإنّ تَمَكُّن أحد المُتسلِّلين من اختراق كلمة المرور الخاصَّة بك على موقع ويب واحد، يعني وصوله إلى عدد من المواقع الأخرى، لذا يُفضَّل تغيير كلمات المرور الخاصَّة بك بانتظام.

3. تَجَنَّب كتابة كلمات المرور الخاصَّة بك في مكان معروف

إنّ كتابة كلمة مرور في أيّ مكان يجعلها عُرْضةً للعثور عليها من قِبل المُتسلِّلين، سواءٌ أكان ذلك على قطعة من الورق، أم في جدول بيانات Excel، أم في تطبيق Notes على هاتفك.

4. المصادقة مُتعدِّدة العوامل

هي أداة تَمْنح مُستخدِمي الإنترنت مستوًى إضافيًّا من أمان الحساب يَتَجَاوَز عنوان البريد الإلكترونيّ بالإضافة إلى مجموعة كلمات المرور، فالمصادقة الثُّنائيَّة تَتَطَلَّب شكلين منفصلين ومتميِّزين لتحديد الهُوِيَّة للوصول إلى شيء ما، والعامل الأوَّل هو كلمة المرور، والثَّاني يتضمَّن عادةً نصًّا يحتوي على رمزٍ يتمّ إرساله إلى هاتفك الذَّكيّ أو بصمة إصبعك أو وجهك أو شبكيَّة العين.

5. التَّقليل من مشاركة البيانات الشَّخصيَّة على وسائل التَّواصل الاجتماعيّ

تَعَرَّف على إعدادات الأمان الخاصَّة بكلّ مِنَصَّة من مِنَصَّات الشَّبكات الاجتماعيَّة وتأكَّد من ضَبْطها على المستوى الذي يُناسِبك لتَجَنُّب الكَشْف عن المعلومات الشَّخصيَّة، مثل عنوانك أو تاريخ ميلادك في السِّيرة الذَّاتية عليها.

6. إغلاق الحسابات غير المُستخدَمة

لقد قام معظمنا بالتَّسجيل في الخدمات عبر الإنترنت، ولم نَعُدْ نَستخدِمها، ومن المحتمل أنَّها تحتوي على مزيج من بياناتك الشَّخصيَّة وتفاصيل هُويَّتك، وكلُّها معلومات قيِّمة لمُجْرمي الإنترنت، والأسوأ من ذلك إذا كنت تَستخدِم نفس كلمة المرور لحسابات مُتعدِّدة؛ لذا يُنْصَح بإزالة بياناتك الخاصَّة من الخدمات التي لم تَعُدْ تَستخدِمها وإغلاق الحسابات القديمة بدلًا من تَرْكها خاملة.

7. حذف المعلومات الشَّخصيَّة الموجودة على وسائط غير آمنة

احْذِف الرَّسائل التي تحتوي على تفاصيل شخصيَّة وراقِبْ بريدك؛ لأنّ ذلك قد يُنَبِّهك إلى حدوث اختراق للبيانات ربَّما لم يتمّ اكتشافه.

8. حافِظ على تحديث الأنظمة والبرامج

وذلك عن طريق تثبيت تحديثات الأمان ومُتصفِّحات الويب وأنظمة التَّشغيل والبرامج بانتظام بمجرَّد توفُّرها.

9. كُن حَذِرًا من خدمة Wi-Fi المجانيَّة

أصْبَح استخدام شبكة Wi-Fi العامَّة المجانيَّة روتينًا يوميًّا لكثير من الأشخاص، ولكنّ الاتِّصالات الآمِنة والموثوقة ليست دائمًا كما تبدو، إذ يمكن أن تكون نقاط اتِّصال Wi-Fi العامَّة أهدافًا سهلةً للمُتسلِّلين ومُجْرمي الإنترنت الذين يمكنهم استخدامها لسرقة البيانات.

10. برامج مُكَافَحَة الفيروسات

من أفضل الطُّرُق للبقاء آمنًا عبر الإنترنت هي استخدام برنامج مكافحة فيروسات عالي الجودة؛ لتحديد نقاط الضَّعف والتَّهديدات في الجهاز، وحَظْر التَّهديدات الإلكترونيَّة قبل أن تَتَرسَّخ.[1]

1. 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe. On Site: https://www.digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-online-safe.

ثالثًا: الوصول غير القانونيّ

تعريف الوصول غير المُصرَّح به (غير القانونيّ)

هو عمليَّة الدُّخول إلى موارد الحاسوب دون إذْنٍ، ويمكن أن يكون نظامًا أو شبكةً أو برنامجًا أو بياناتٍ، وعادةً ما يتمّ ارتكاب الوصول غير المُصرَّح به من قِبل المُتسلِّلين، وأحيانًا المُستخدِمين غير المُتعمِّدين، فيمكن لأيّ شخص لديه إمكانيَّة الوصول بالفعل إلى النِّظام أن يَعْثُر بطريق الخطأ على ملفَّات غير آمِنة لم تكن مُخصَّصة للمُعاينة.

أمَّا عن كيفيَّة وصول الأشخاص غير المُصرَّح لهم إلى الأنظمة والملفَّات فأسبابه:

- قيام المُستخدِم عن طريق الخطأ بتخمين كلمة مرور لملفَّات أو بيانات حسَّاسة.
- تنفيذ هجمات مُعقَّدة تستغرق أسابيع من التَّخطيط، وقد تتضمَّن حتى تجسُّسًا على المؤسَّسات والمُستخدِمين.
- يمكن لمُجْرمي الإنترنت أن يذهبوا إلى أبعد من ذلك في خداعهم لاكتساب ما يكفي من الثِّقة ليكونوا أشخاصًا مُرخَّصًا لهم.

مخاطر الوصول غير المُصرَّح به

1. تعطيل الأنظمة الإلكترونيَّة.
2. إيذاء الهدف؛ فعادةً ما تكون البيانات غير المُصرَّح بها حسَّاسة ويمكن أن تُلْحِق الضَّرر بالضَّحيَّة.
3. سرقة البيانات، وهي الطَّريقة الأكثر شيوعًا التي قد يرغب شخصٌ ما في الوصول بها إلى البيانات غير المُصرَّح بها؛ لاستخدامها في الحصول على فِدْيَة.
4. يُسبِّب أضرارًا ماديَّة للأجهزة المتَّصلة بالشَّبكة.
5. الإضْرار بسمعة المؤسَّسات والأفراد.
6. العقوبات الماليَّة والمعنويَّة؛ حيث تحتاج كثير من المؤسَّسات إلى الالْتِزام بمجموعة مُحدَّدة من الإجراءات واللَّوائح الأمنيَّة عبر الإنترنت، ومع وصول مُجْرمي الإنترنت غير المُصرَّح لهم إلى أنظمة وملفَّات هذه المؤسَّسات فإنّ إمكانيَّة تَعَرُّض العملاء للضَّرر تزيد، وبالتَّالي تتضرَّر سمعة المؤسَّسة وقد تَتَعرَّض لغرامة من جرَّاء ذلك.
7. تزايد التَّكاليف، فرغبة المؤسَّسات في إصلاح الثَّغرات والأعطال النَّاتجة عن الوصول غير المُصرَّح به لأنظمتها وملفَّاتها تدفعها إلى دَفْع مزيد من التَّعويضات والتَّكاليف التي تَصِل إلى عشرات الملايين من الدُّولارات.[1]

أمثلة على الوصول غير المُصرَّح به

1. سرقة بطاقة الدُّخول الخاصَّة بشخصٍ ما من النَّاحية الفَنِّيَّة بمنزلة وصول غير مُصرَّح به؛ إذ يمكن للمُجْرم بعد ذلك سرقة أجهزة الحاسوب المحمولة الخاصَّة بالمكتب أو إتلاف أيّ إطار حاسوب فعليًّا.
2. استغلال الثَّغرات الأمنيَّة؛ إذ يميل المُتسلِّلون إلى أن يكونوا ماهرين وصبورين من خلال الاستكشاف الدَّقيق للشَّبكة الرَّقميَّة للأفراد والمؤسَّسات لمعرفة نقاط الضَّعف واستغلالها.
3. الهندسة الاجتماعيَّة، ويُقصَد بها خداع شخصٍ ما للقيام بشيءٍ ضارٍّ بنفسه أو بأجهزته، وكلّ ما يتطلَّبه الأمر هو بريد إلكترونيّ مدروس ومُصمَّم جيِّدًا أو موقع ويب مكرَّر لخداع شخصٍ ما للتَّخلّي عن اسم المُستخدِم وكلمة المرور الخاصَّة به.

1. What is unauthorized access? nordvpn. On Site: https://nordvpn.com/blog/unauthorized-access/.

نصائح لاكتشاف الدُّخول غير المُصرَّح به ومَنْعه

1. وَضْع كلمة مرور قويَّة ومُعقَّدة وتغييرها من حين إلى آخر

لا ينبغي لك أبدًا استخدام كلمة "password" ككلمة مرور فحسب، بل إنَّها أيضًا كلمة المرور الأكثر استخدامًا في الوقت نفسه، وبهذا لا يحتاج المُتسلِّل أقلّ من ثانية لمعرفة بعض كلمات المرور الأكثر شيوعًا، ويُفضَّل عدم استخدام تواريخ الميلاد أو أيّ شيء يُحدِّد هُوِيَّتك أو عائلتك.

2. التَّذكير والفحوص المُنتظِمة بشأن الممارسات الأمنيَّة

أفضل طريقة للتَّدرُّب على الممارسات الجديدة هي الرُّوتين، إذ إنّ التَّذكير البسيط لجميع المُستخدِمين بالممارسات الأمنيَّة بانتظام يُعزِّز الأمن السِّيبرانيّ بشكلٍ كبيرٍ.

3. تخزين البيانات الذَّكيَّة

من الطُّرُق الأكثر فاعليَّة لمَنْع الوصول غير المُصرَّح به هي تقليل عدد الأجهزة التي يمكنها الوصول إلى البيانات الحسَّاسة، مثل إزالة قُدْرة الأجهزة المحمولة مثل الهواتف أو الأجهزة اللَّوحيَّة على الوصول إلى أجزاء معيَّنة من الشَّبكة.

4. مُراقَبَة النَّشاط الرَّقميّ على الإنترنت

إنّ كثيرًا من خروقات البيانات والأضرار النَّاجمة عن حصول شخصٍ ما على وصولٍ غير مُصرَّحٍ به تأتي من مُستخدِمين داخليِّين؛ بهدف التَّجسُّس الكامل بقَصْد التَّسبُّب في أكبر قَدْرٍ ممكنٍ من الضَّرر، لذا فإنّ مراقبة نشاط المُستخدِم تَجْعَل من السَّهْل اكتشاف العلامات الواضحة لشخص يَتطلَّع إلى التَّسبُّب في الفوضى.

5. قُمْ بتأمين جميع نقاط النِّهاية

نقطة النِّهاية هي أيّ مكان يمكن للمُستخدِم من خلاله الوصول إلى شبكة الحاسوب أو النِّظام، ويُفضَّل تثبيت برنامج مُكَافَحَة الفيروسات على كلّ نقطة نهاية لاكتشاف البرمجيَّات الضَّارة وإزالتها.[1]

1. Detecting and Responding to Unauthorized Access. Top 8 Practices to Implement, June 28, 2023. On Site: https://www.ekransystem.com/en/blog/detecting-and-responding-to-unauthorized-access.

رابعًا: البرمجيّات الضَّارَّة

تعريف البَرمَجيّات الضَّارَّة

هـو مصطلـح شـامل يَصِـف أيّ بَرمَجيّـات أو تعليمـات برمجيّـة ضـارَّة تَضُـرّ بالأنظمـة، فهـي تسـعى عـن عَمْـد إلـى غَـزْو أجهـزة الحاسـوب وأنظمتهـا والشَّبكات والأجهـزة اللَّوحيَّة والأجهـزة المحمولة بهدف إتلافها أو تعطيلها، وذلـك غالبًـا عـن طريـق التَّحكُّـم الجزئـيّ فـي عمليّـات الجهـاز.

وتختلـف الدَّوافـع وراء البَرمَجيّـات الضَّـارَّة، إذ يمكـن أن تهـدف إلـى جَنْـي الأمـوال منـك، أو تخريـب قُدْرَتـك علـى إنجـاز العمـل، أو مجـرَّد التَّفاخـر، ولا يمكن للبَرمَجيّـات الضَّـارَّة إتـلاف الأجهـزة المادِّيَّـة للأنظمـة أو مُعـدَّات الشَّـبكة، إلَّا أنَّهـا يمكنهـا سـرقة بياناتـك أو تَشْـفيرها أو حَذْفهـا، أو تَغْيير وظائـف الحاسـوب الأساسـيَّة أو الاسـتيلاء عليهـا، والتَّجسُّـس علـى نشـاط الحاسـوب الخـاصّ بـك دون عِلْمـك أو إذْنـك.[1]

كيـف يمكننـي معرفـة مـا إذا كان جِهـازي مصابًـا بعـدوى البَرمَجيّـات الضَّـارَّة؟

يمكـن أن تَكْشِـف البَرمَجيّـات الضَّـارَّة عـن نفسـها مـن خـلال عـدد مـن السُّـلوكيَّات الشَّـاذَّة المختلفـة، وفيمـا يلـي بعـض العلامـات التـي تشـير إلـى وجـود بَرمَجيّـات ضـارَّة علـى نظامـك:

1. بُـطْء جهـاز الحاسـوب الخـاصّ بـك؛ حيـث تَقِـلّ سـرعة نظـام التَّشـغيل لديـك، سـواءٌ أكنـت تتصفَّـح الإنترنـت أم تَسـتخدِم تطبيقاتـك المحلِّيَّـة فقـط، فـإنّ اسـتخدام مـوارد نظامـك يبـدو مرتفعًـا بشـكلٍ غيـر طبيعـيّ، وقـد تُلاحـظ أيضًـا أنّ مروحـة جهـاز الحاسـوب الخـاصّ بـك تعمـل بأقصـى سـرعة، وهـو مُؤشِّـر علـى أنّ شـيئًا مـا يَسْـتهلِك مـوارد النِّظـام فـي الخلفيَّـة، ويحـدث هـذا عـادةً عندمـا يكـون جهـاز الحاسـوب الخـاصّ بـك مُقيَّـدًا بشـبكة الرُّوبوتـات.

2. شاشـتك ملآنـة بالإعلانـات المزعجـة، فالإعلانـات المُنبثِقـة غيـر المُتوقَّعـة علامـة نموذجيَّـة علـى الإصابـة بالبَرمَجيّـات الضَّـارَّة، فهـي مرتبطـة بشـكلٍ خـاصّ بنـوع مـن البَرمَجيّـات الضَّـارَّة المعروفـة باسـم بَرمَجيّـات الإعلانـات المُتسلِّلة، وعـادةً مـا تأتـي النَّوافـذ المُنبثِقـة مُحَمَّلـة بتهديـدات البَرْمَجيّـات الضَّـارَّة المخفيَّـة الأخـرى.

1. ما المقصود بالبَرمَجيّات الضَّارَّة؟ support.google.com. متاح على الرَّابط: https://support.google.com/google-ads/answer/2375413?hl=ar.

3. تَعَطُّل النِّظام الخاصّ بك، ويأتي هذا على شكل تجميد أو شاشة الموت الزَّرقاء (BSOD)، ويحدث هذا الأخير على أنظمة Windows بعد مواجهة خطأ فادح.

4. فقدانٌ غامضٌ لمساحة القُرْص، وسببه وجود بَرمَجيَّات ضارَّة متضخِّمة، مختبئة في مُحرِّك الأقراص الثَّابتة لديك والمعروفة أيضًا باسم البَرمَجيَّات المُجمَّعة.

5. زيادةٌ غريبةٌ في نشاط الإنترنت لنظامك، فعلى سبيل المثال بمجرَّد وصول حصان طروادة إلى جهاز حاسوب مُستهدَف، فإنّ الشيء التَّالي الذي يفعله هو الوصول إلى خادم القيادة والتَّحكُّم (C&C) الخاصّ بالمُهاجِم لتنزيل عدوى ثانويَّة، وغالبًا ما تكون بَرمَجيَّات فِدْيَة، ما يُفسِّر الارتفاع الكبير في نشاط الإنترنت.

6. تتغيَّر إعدادات المُتصفِّح بشكلٍ تلقائيٍّ، فإذا لاحَظْت تغييرًا في صفحتك الرَّئيسة أو كان لديك أشرطة أدوات أو مُلْحَقات أو مُكوِّنات إضافيَّة جديدة مُثَبَّتة، فقد يكون لديك نوع من الإصابة بالبَرمَجيَّات الضَّارَّة.

7. يتوقَّف برنامج مُكَافَحَة الفيروسات عن العمل ولا يمكنك تشغيله مرَّة أخرى، ما يتركك غير محميّ ضدّ البَرمَجيَّات الضَّارَّة الخادعة التي عَطَّلَتْه.

8. فقدان إمكانيَّة الوصول إلى ملفَّاتك أو جهاز الحاسوب بأكمله، وهذا من أعراض الإصابة بِبَرمَجيَّات الفِدْيَة.[1]

ولا بُدّ هنا من الإشارة إلى إمكانيَّة اختباء البَرمَجيَّات الضَّارَّة القويَّة في جهاز الحاسوب الخاصّ بك دون اكتشافها، ويحدث الحصول على البَرمَجيَّات الضَّارَّة عبر طريقتين هما الأكثر شيوعًا: الإنترنت والبريد الإلكترونيّ؛ لذا في أيّ وقت تكون فيه متَّصلًا عبر الإنترنت، تكون عُرْضةً للخَطَر؛ وبشكلٍ عامٍّ لن تنجح هجمات البَرمَجيَّات الضَّارَّة من دون فِعْل المُستخدِم المُستهدَف سلوكيَّات تُسَهِّل عمليَّة الاختراق، مثل فَتْح مُرْفَق بريد إلكترونيّ لا تعرفه، أو النَّقْر على شيءٍ ما وتَثْبيته من مصدر غير جدير بالثِّقة.

أنواع البَرمَجيَّات الضَّارَّة

للبَرمَجيَّات الضَّارَّة أنواع عدَّة، فيما يلي تبيان لأهمِّها

1. بَرمَجيَّات الإعلانات المُتسلِّلة

هي بَرمَجيَّات غير مرغوب فيها مُصمَّمة لعَرْض الإعلانات على شاشتك، وغالبًا ما تكون داخل مُتصفِّح الويب، وتَستخدِم أسلوبًا مخادعًا، إمَّا لإخفاء نفسها كبرنامج شرعيّ، وإمَّا استغلالها في برنامج آخر لخداعك لتثبيته على جهاز الحاسوب أو الجهاز اللَّوْحيّ أو الجهاز المحمول.

2. بَرمَجيَّات التَّجسُّس

هي بَرمَجيَّات ضارَّة تُراقِب سرًّا أنشطة مُستخدِم الحاسوب دون إذْنٍ وتقوم بإبلاغ مؤلِّف البرنامج عنها.

3. الفيروس

هو برنامج ضارّ يرتبط ببرنامج آخر، وعند تنفيذه عن غير قَصْد من قِبل المُستخدِم يُكرِّر نفسه عن طريق تعديل برامج الحاسوب الأخرى وإصابتها بأجزاء من التَّعليمات البرمجيَّة الخاصَّة به.

4. الدِّيدان

هي نوع من البَرمَجيَّات الضَّارَّة تُشْبِه الفيروسات التي تتكاثر ذاتيًّا وتَنْتَشِر عبر الأنظمة من تِلْقاء نفسها.

5. حصان طروادة

أحد أخطر أنواع البَرمَجيَّات الضَّارَّة، وعادةً ما يُمثِّل نفسه على أنَّه شيء مفيد لخداعك، وبمجرَّد وصوله إلى نظامك يَحْصُل المُهاجِمون الذين يقفون وراء حصان طروادة على وصولٍ غير مُصرَّحٍ به إلى الحاسوب المصاب؛ لسرقة المعلومات الماليَّة أو تثبيت أشكال أخرى من البَرمَجيَّات الضَّارَّة، وغالبًا ما تكون بَرمَجيَّات الفِدْيَة.

6. بَرمَجيَّات الفِدْيَة

هي أحد أشكال البَرمَجيَّات الضَّارَّة التي تَمْنَعك من الوصول إلى جهازك أو تقوم بتشفير ملفَّاتك، ثمّ تُجْبِرك على دَفْع فِدْيَة لاستعادة الوصول.

7. بَرمَجيَّات الاستغلال

هي نوع من البَرمَجيَّات الضَّارَّة التي تستغلّ الأخطاء ونقاط الضَّعف في النِّظام لمَنْح المُهاجِم حقّ الوصول إلى نظامك.[1]

1. The 12 Most Common Types of Malware, Kurt Baker - February 28, 2023. On Site: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

كيفيَّة إزالة البَرمَجيَّات الضَّارَّة

اتَّبِع هذه الخطوات الثَّلاثة السَّهلة لإزالة البَرمَجيَّات الضَّارَّة من جهازك:

1. ثَبِّت وحَمِّل برنامجًا جيِّدًا لمُكافَحَة البَرْمَجيَّات الضَّارَّة.
2. أجْرِ فَحْصًا باستخدام برنامجك الجديد.
3. غَيِّر جميع كلمات المرور الخاصَّة بك.

كيفيَّة الحماية من البَرمَجيَّات الضَّارَّة

1. انْتَبِه إلى النِّطاق وكُن حَذِرًا إذا لم يكُن الموقع نطاقًا من المستوى الأعلى، مثل com أو mil أو net أو org أو edu أوbiz، على سبيل المثال لا الحصر.
2. اسْتَخدِم كلمات مرور قويَّة مع مصادقة مُتعدِّدة العوامل.
3. تَجَنَّب النَّقْر على الإعلانات المُنبثِقة في أثناء تَصَفُّح الإنترنت.
4. تَجَنَّب فَتْح مُرْفَقات البريد الإلكترونيّ من المُرسِلين غير المعروفين.
5. لا تَنْقُر على الرَّوابط الغريبة، التي لم يتمّ التَّحقُّق منها في رسائل البريد الإلكترونيّ والنُّصوص ورسائل وسائل التَّواصل الاجتماعيّ.
6. لا تُنَزِّل التَّطبيقات من مواقع الويب غير الجديرة بالثِّقة.
7. الْتَزِم بالتَّطبيقات الرَّسميَّة من Google Play وApp Store على أنظمة Android وOSX وiOS.
8. تأكَّد من أنّ نظام التَّشغيل والمُتصفِّحات والمُكوِّنات الإضافيَّة لديك مُصحَّحة ومُحدَّثة.
9. احْذِف أيّ برامج لم تَعُدْ تستخدمها.
10. قُمْ بعمل نسخة احتياطيَّة لبياناتك بانتظام.
11. ثَبِّت تطبيقًا حديثًا لمكافحة البرمجيَّات الضَّارَّة، بهدف فحص التَّهديدات ومَنْعِها من الوصول إلى جهازك.[1]

1. كيفيَّة حماية الجهاز من البرمجيَّات الخبيثة، salamatechwiki. مُتاح على الرَّابط: https://cutt.us/ssynj.

الفَصْل الثَّالث

حماية الأجهزة من الأخطار الرَّقميَّة

- أوَّلًا: كلمات المرور
- ثانيًا: النَّسْخ الاحتياطيّ للبيانات

0 3

أوَّلًا: كلمات المرور

ما الحماية بكلمة المرور؟

تُساعِد الحماية بكلمة مرور على حماية بياناتك من الجِهات الفاعلة السَّيِّئة، من خلال اكتشاف كلمات المرور الضَّعيفة المعروفة والمصطلحات الضَّعيفة الخاصَّة بك وحَظْرها، فهي تقنيَّة للتَّحكُّم في الوصول تُساعِد في الحفاظ على البيانات المهمَّة آمِنةً من المُتسلِّلين، من خلال ضمان عدم إمكانيَّة الوصول إليها إلَّا باستخدام بيانات الاعتماد الصَّحيحة.[1]

أهمِّيَّة حماية كلمة المرور

تُعَدّ حماية كلمة المرور إحدى أدوات أمان البيانات الأكثر شيوعًا المتاحة للمُستخدِمين، فهي خطّ الدِّفاع الأوَّل ضدّ الوصول غير المُصرَّح به إلى الحسابات والأجهزة والملفَّات عبر الإنترنت، وتُساعِد كلمات المرور القويَّة على حماية البيانات من العناصر السَّيِّئة والبَرمَجيَّات الضَّارَّة، فكلَّما كانت كلمة المرور أقوى؛ زادت حماية المعلومات.

عواقب استخدام كلمات المرور الضَّعيفة

بالنِّسبة للأفراد، يمكن أن يكون لفقدان المعلومات الشَّخصيَّة تداعيات ماليَّة وتداعيات على السُّمعة طويلة الأمد، وعندما يحصل مُجْرمو الإنترنت على وصولٍ غير مُصرَّحٍ به إلى بيانات المؤسَّسة، يمكن أن تَتَعَرَّض لخسارة كبيرة في الإيرادات والمِلْكِيَّة الفِكْرِيَّة وتعطيل العمليَّات، فضلًا عن تَكَبُّد غرامات تنظيميَّة والإضرار بالسُّمعة.

1. What is password protection? Microsoft. On Site: https://www.microsoft.com/en-us/security/business/security-101/what-is-password-protection.

إرشادات عامَّة لإنشاء كلمات مرور قويَّة

1. اسْتَخدِم ما لا يقلّ عن 12 حرفًا.
2. اسْتَخدِم مزيجًا من الحروف والأرقام والرُّموز.
3. اسْتَخدِم حرفًا كبيرًا واحدًا على الأقلّ.
4. اسْتَخدِم كلمة مرور مختلفة لكلّ حساب من حساباتك، واعمل على تغيير كلمة المرور بين الحين والآخر.
5. اسْتَخدِم كلمات غير مألوفة وغير عاديَّة، مثل كلمات الأغاني أو الاقتباسات أو العبارات الشَّائعة، لجَعْل كلمة المرور أكثر سهولة عند التَّذَكُّر، مثل استخدام أوَّل حرفين من كلّ كلمة في الجملة.

بعض الأمثلة على كلمات المرور الضَّعيفة

1. 1234567.
2. 1111111.
3. كلمة المرور 123.
4. QWERTY.

ثانيًا: النَّسْخ الاحتياطيّ للبيانات

يُعَدّ وجود خطَّة لعمل نسخة احتياطيَّة من البيانات إحدى أهمّ العمليَّات لحماية البيانات في حالة وقوع هجوم إلكترونيّ، سواءٌ هجوم ببرنامج ضارٍّ أم ببرنامج فِدْيَة، إذ يمكنك تشغيل نسخة احتياطيَّة محفوظة واستعادة بياناتك بحالتها السَّابقة، ويمكن الاستفادة من حُلول التَّخزين السَّحابيَّة، مثل: Google Drive أو Dropbox، أو من خلال نَسْخها على مُحرِّك أقراص ثابت خارجيّ.

إستراتيجيَّات فعَّالة لإجراء نَسْخ احتياطيّ آمِن لبياناتك

1. قاعدة 3-2-1

يُقصَد بها إنشاء 3 نُسَخ مختلفة من بياناتك لوَضْعها على نوعين مختلفين من وحدات التَّخزين والاحتفاظ بنسخة واحدة خارج الموقع، **وهناك عدَّة طُرُق لذلك فيما يلي تبيان لها:**

- استخدام مُحرِّك أقراص ثابت خارجيّ ويتمّ ذلك عبر استخدام برنامج النَّسْخ الاحتياطيّ المُدْمَج في جهاز الحاسوب الخاصّ بك لعمل نسخة احتياطيَّة لملفَّاتك على جهاز تخزين خارجيّ، كلّ ما عليك فِعْله هو توصيل مُحرِّك الأقراص الخارجيّ بجهاز الحاسوب الخاصّ بك وسيقوم البرنامج بالباقي.
- استخدام برنامج نَسْخ احتياطيّ تَابِع لجِهة خارجيَّة، وتكون هذه البرامج في بعض الأحيان أسرع وأكثر كفاءة لأنَّها تَستخدِم البرامج السَّحابيَّة.
- نَسْخ الملفَّات يدويًّا، تستغرق عمليَّة نَقْل البيانات يدويًّا وقتًا أطول، ولكنَّه يُعَدّ خيارًا جيِّدًا إذا كنت لا تريد استخدام برنامج النَّسْخ الاحتياطيّ.

2. اسْتَخدِم مُحرِّك أقراص فلاش USB؛ تُعَدّ مُحرِّكات أقراص USB المحمولة حلول تخزين محمولة رائعة لتخزين أهمّ الملفَّات من جهاز الحاسوب الخاصّ بك؛ لأنّ مُحرِّكات أقراص USB عادةً ما تكون أصغر بكثير من مُحرِّكات الأقراص الثَّابتة الخارجيَّة.

3. اسْتَخدِم الوسائط البصريَّة، مثل الأقراص المضغوطة أو أقراص DVD لعمل نسخة من بياناتك، وهي طريقة فعَّالة لأنَّها تُوفِّر نسخة احتياطيَّة فعليَّة لبياناتك التي يمكنك الاحتفاظ بها في مكان آمِن.

4. اسْتَخدِم التَّخزين السَّحابيّ؛ إذ يُعَدّ طريقة جيِّدة لإنشاء نُسَخ احتياطيَّة كنوع من الوسائط عبر الإنترنت، ويمكن لهذه الخدمة تخزين الملفَّات أو الصُّور أو أيّ نوع آخر من البيانات، إذ تُوفِّر لك خدمة التَّخزين السَّحابيّ قَدْرًا معيَّنًا من المساحة على خوادمها مقابل رسوم شهريَّة، ويمكنك الوصول إلى النُّسْخة الاحتياطيَّة السَّحابيَّة من أيّ جهاز حاسوب أو جهاز محمول متَّصل بالإنترنت، ويمكنك استخدام مُوفِّري التَّخزين السَّحابيّ، مثل: Google Drive وiCloud وDropbox وBackb.

5. اسْتَخدِم خدمة النَّسْخ الاحتياطيّ عبر الإنترنت؛ يمكن عَمَل نسخة احتياطيَّة لبياناتك باستخدام خدمة النَّسْخ الاحتياطيّ عبر الإنترنت عن طريق تَشْفير ملفَّاتك، وجَدْوَلة النُّسَخ الاحتياطيَّة المُنتظِمة، وتخزين ملفَّات النَّسْخ الاحتياطيّ في مكان آمِن.

6. جهاز تخزين متَّصل بالشَّبكة (NAS): هو خادم مُخصَّص يُوفِّر تخزينًا ومشاركة على مستوى الملفّ لشبكة منزلك أو شركتك الصَّغيرة، وهو قَيْد التَّشغيل والاتِّصال دائمًا؛ حتى تتمكَّن من الوصول إلى بياناتك في أيّ وقت ومن أيّ مكان.[1]

وعمومًا، تحميك النُّسَخ الاحتياطيَّة من فقدان البيانات في حال تَعَطَّل جهاز الحاسوب الخاصّ بك أو فَشِل مُحرِّك الأقراص الثَّابتة لديك، كما تحميك من البَرمَجيَّات الضَّارَّة وبَرمَجيَّات الفِدْيَة إذا أُصِيب جهاز الحاسوب الخاصّ بك بها، لكن عليك الحِفاظ على خطَّة النَّسْخ الاحتياطيّ الخاصَّة بك مُحدَّثة.

1. Kyle Chinj How to Back Up Your Data: 6 Effective Strategies to Prevent Data Loss, 2023. On Site: https://www.upguard.com/blog/how-to-back-up-your-data.


البطاقات التّدريبيّة

انْتَبِه!

جهاز التخزين (NAS)

هو جِهاز مُخصّص يُوفِّر تخزينًا ومشاركة على مستوى الملفّ لشبكة منزلك أو شركتك الصَّغيرة، وهو قَيْد التَّشغيل والاتِّصال دائمًا؛ حتى تتمكَّن من الوصول إلى بياناتك في أيّ وقت ومن أيّ مكان.

انْتَبِه!

قاعدة 3-2-1

يُقصَد بها إنشاء 3 نُسَخ مختلفة من البيانات لوَضْعها على نوعين مختلفين من وحدات التَّخزين والاحتفاظ بنسخة واحدة خارج الموقع، وهناك عدَّة طُرُق لذلك:

- اسْتَخدِم مُحرِّك أقراص ثابت خارجيّ.
- اسْتَخدِم برنامج نَسْخ احتياطيّ تابِع لجهة خارجيَّة، مثل البرامج السَّحابيَّة.
- نَسْخ الملفَّات يدويًّا.

انْتَبِه!

تعريف البرمجيّات الضارة

هو مصطلح شامل يَصِف أيّ برنامج أو تعليمات برمجيَّة ضارَّة تَضُرّ بالأنظمة، فهي تسعى عن عَمْد إلى غَزْو أجهزة الحاسوب وأنظمتها والشَّبكات والأجهزة اللَّوحيَّة والأجهزة المحمولة بهدف إتلافها أو تعطيلها، وذلك غالبًا عن طريق التَّحكُّم الجزئيّ في عمليَّات الجهاز.

انْتَبِه!

الوصول غير المُصرَّح به (غير القانونيّ)

هو عمليّة الدُّخول إلى موارد الحاسوب دون إذْنٍ، ويمكن أن يكون نظامًا أو شبكةً أو برنامجًا أو بياناتٍ، وعادةً ما يتمّ ارتكاب الوصول غير المُصرَّح به من قِبل المُتسلِّلين، وأحيانًا المُستخدِمين غير المُتعمِّدين، فيمكن لأيّ شخص لديه إمكانيَّة الوصول بالفعل إلى النِّظام أن يَعْثُر بطريق الخطأ على ملفَّات غير آمِنة لم تكن مَخصَّصة للمُعاينة.

كيفيَّة الحفاظ على البيانات آمِنة

انْتَبِه!

1. اسْتَخدِم كلمات مرور قويَّة وتغييرها بين الحين والآخر.
2. تَجَنَّب استخدام نفس كلمة المرور لحسابات متُعدِّدة.
3. تَجَنَّب كتابة كلمات المرور الخاصَّة بك في أيّ مكان.
4. المصادقة مُتعدِّدة العوامل.
5. كُن حَذِرًا عند مشاركة المعلومات الشَّخصيَّة.
6. الحدّ من مشاركة وسائل التَّواصل الاجتماعيّ.
7. إغلاق الحسابات غير المُستخدَمة على الإنترنت.
8. حافِظ على تحديث الأنظمة والبرامج.
9. كُن حَذِرًا من خدمة Wi-Fi المجانيَّة.
10. اسْتَخدِم برامج مُكَافَحَة الفيروسات.

انْتَبِه!

سرقة البيانات

هي نَقْل أو تَخْزين غير قانونيّ للمعلومات الشَّخصيَّة أو السِّرِّيَّة أو الماليَّة، ويمكن أن يشمل ذلك كلمات المرور أو التَّعليمات البرمجيَّة أو الخوارزميَّات البرمجيَّة والعمليَّات أو التِّقنيَّات الخاصَّة، وتُمثِّل انتهاكًا خطيرًا للأمان والخصوصيَّة.

انْتَبِه!

برمجيّات الفِدْيَة
Ransomware

عبارة عن برمجيّات ضارّة مُصمّمة لمَنْع المُستخدِم أو المؤسّسة من الوصول إلى الملفّات الموجودة على أجهزة الحاسوب الخاصّة بهم، للمُطالَبة بدَفْع فِدْيَة مقابل استعادة الوصول إلى ملفّاتهم.

انْتَبِه!

أمن المعلومات Information Security

يُقصَد به الوسائل والأدوات والإجراءات اللّازم توفيرها لضمان حماية المعلومات من الأخطار الدّاخليّة والخارجيّة، وهو العِلْم الذي يَدْرُس كيفيّة توفير تدابير حماية سرّيّة وسالمة للمعلومات وكيفيّة مُكَافَحَة الاعتداء عليها.

انْتَبِه!

أمن الشَّبكات

هو جزء من منظومة أمن المعلومات التي تقوم على حماية استخدام الشَّبكة وسلامتها، ومِن ثَمَّ سلامة عمليَّات نَقْل وتَبادُل البيانات، ويشمل هذا المجال كلًّا من تكنولوجيا الأجهزة والتَّطبيقات، ويَستهدِف مجموعةً مُتنوِّعةً من التَّهديدات ويَمْنَعُها من الدُّخول إلى شبكتك أو من الانتشار.


الإكتشات

أبرز المَخاطِر الرَّقميَّة التي تواجه الأجهزة الرَّقميَّة (الحواسيب، الهواتف الذَّكيَّة، الأجهزة اللَّوحيَّة)

01 تَسَرُّب البيانات.

02 تزوير الشَّبكة.

03 هجمات التَّصيُّد الاحتياليّ.

04 برمجيَّات التجسس.

كيفيَّة عمل بَرْمَجيَّات الفِدْيَة

هناك ثلاث مراحل أساسيَّة تَمُرّ بها هذه العمليَّة

- ناقلات العدوى والتَّوزيع.
- تشفير البيانات.
- طَلَب الفِدْيَة.

كيف يمكن الحماية من برمجيّات الفِدْيَة؟

1. التّوعية والتّأهيل والتّدريب على مفاهيم الأمن السّيبرانيّ والسّلامة الرّقميّة.
2. النّسْخ الاحتياطيّ المستمرّ للبيانات.
3. تصحيح الثّغرات في الأنظمة التي لم تُصحّح بعد.
4. تُعَدّ مصادقة المُستخدِم وسيلةً مهمّةً لمَنْع المُهاجِم من الاستفادة من كلمة المرور التي تمّ تخمينها أو سرقتها.
5. تقليل سَطْح الهجوم، ويتمّ ذلك عن طريق معالَجة الآتي

- رسائل التّصيُّد.
- نقاط الضّعف غير المُصحّحة.
- حلول الوصول عن بُعْد.
- البَرمَجيّات الضّارّة للأجهزة الذّكيّة


كيف تُخَفِّف من عدوى برمجيّات الفِدْيَة النَّشطة؟
عَزْل الجهاز.
اتْرُك الحاسوب قَيْد التَّشغيل.
إنشاء نسخة احتياطيّة من الملفّات.
التَّحقُّق من وجود أدوات فكّ التَّشفير.
اطْلُب المساعدة من شخص مُتخصِّص.
المَسْح والاستعادة عبر تثبيت نظام التَّشغيل لضمان إزالة البَرْمَجيَّات الضَّارَّة بالكامل من الجهاز.

كيف تحدث سرقة البيانات؟

تحدث من خلال مجموعة مُتنوِّعة من الوسائل

1. **الهندسة الاجتماعيَّة.**
2. **كلمات المرور الضَّعيفة.**
3. **نقاط ضعف النِّظام** (الثَّغرات الأمنيَّة).
4. **التَّهديدات الدَّاخليَّة** من قِبل بعض المُوظَّفين الذين يعملون في مؤسَّسة ما للوصول إلى المعلومات الشَّخصيَّة للعملاء واستغلالها.
5. **خطأ بشريّ.**
6. **تثبيت البرامج من مواقع غير موثوقة.**
7. **سرقة الأجهزة الإلكترونيَّة أو ضياعها.**
8. **المعلومات المتاحة للجمهور.**

نصائح لاكتشاف الدُّخول غير المُصرَّح به ومَنْعه

1. وَضْع سياسة كلمة مرور قويَّة ومُعقَّدة وتغييرها بين الحين والآخر.
2. التَّذكير والفحوص المُنتظِمة بشأن الممارسات الأمنيَّة عبر التَّدريب.
3. تقليل عدد الأجهزة التي يمكنها الوصول إلى البيانات الحسَّاسة.
4. تأمين جميع نقاط النِّهاية عبر تثبيت برنامج مُكَافَحَة الفيروسات على كلّ نقطة نهاية؛ لاكْتِشَاف البَرْمَجيَّات الضَّارَّة وإزالتها.

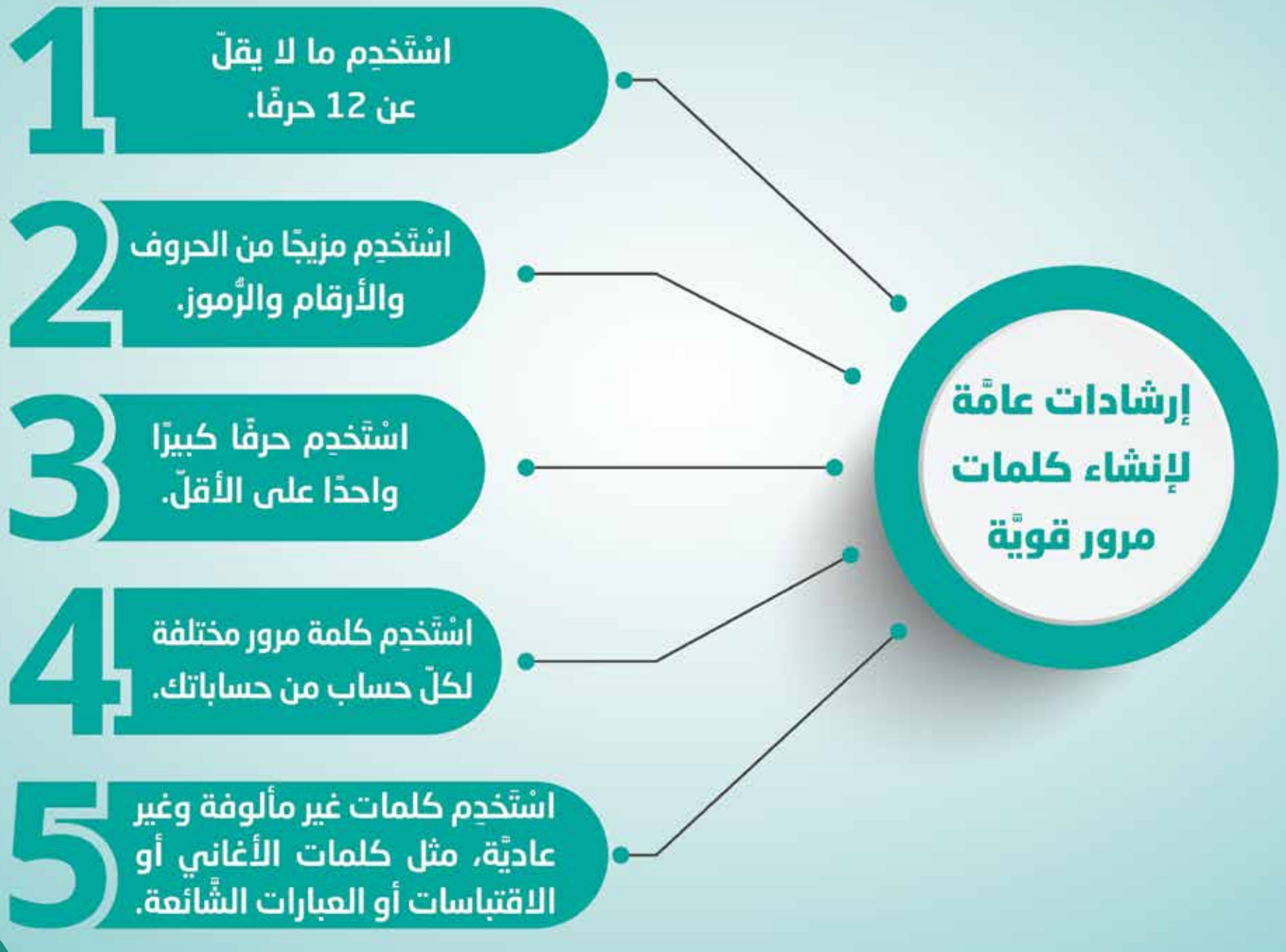
كيف يمكنني معرفة ما إذا كان جهازي مصابًا بعدوى البرمجيّات الضّارّة؟

- بُطْء جهاز الحاسوب الخاصّ بك.
- ظهور الإعلانات المُزعِجة على الشّاشة.
- تَعَطُّل نظام التّشغيل، ويأتي هذا على شكل تجميد أو شاشة الموت الزّرقاء (BSOD)، ويحدث هذا الأخير على أنظمة Windows.
- فقدانٌ غامضٌ لمساحة القُرْص.
- زيادةٌ غريبةٌ في نشاط الإنترنت لنظامك.
- تَغَيُّر إعدادات المُتصفِّح الخاصّ بك.
- تَوقُّف برنامج مُكَافَحَة الفيروسات الخاصّ بك عن العمل.
- فقدان إمكانيّة الوصول إلى ملفّاتك أو جهاز الحاسوب بأكمله.

كيفيّة إزالة البرمجيّات الضّارّة

أهمِّيَّة حماية كلمة المرور

هي خطّ الدِّفاع الأوَّل ضدّ الوصول غير المُصرَّح به إلى الحسابات والأجهزة والملفَّات عبر الإنترنت، وتُساعِد كلمات المرور القويَّة على حماية البيانات من العناصر السيئة والبرمجيَّات الضارة، فكلَّما كانت كلمة المرور أقوى؛ زادت حماية المعلومات.


إرشادات عامّة
لإنشاء كلمات
مرور قويّة
1
اسْتَخدِم ما لا يقلّ
عن 12 حرفًا.
2
اسْتَخدِم مزيجًا من الحروف
والأرقام والرُّموز.
3
اسْتَخدِم حرفًا كبيرًا
واحدًا على الأقلّ.
4
اسْتَخدِم كلمة مرور مختلفة
لكلّ حساب من حساباتك.
5
اسْتَخدِم كلمات غير مألوفة وغير
عاديّة، مثل كلمات الأغاني أو
الاقتباسات أو العبارات الشّائعة.

مراجـــــــع

المحتوى العلمي

في الحـــــــقيبة

المراجع العربيَّة:

1. إبراهيم، حمادي عثمان. أمن المعلومات، محاضرات مادَّة الحاسوب، قسم اللُّغة الإنجليزيَّة، كلِّيَّة التَّربية للعلوم الإنسانيَّة، جامعة الأنباء، العراق. متاح على الرَّابط: https://www.uoanbar.edu.iq/eStoreImages/Bank/1352.pdf.
2. بَرمَجيَّات الفدية - التعريف والوقاية منها وإزالتها، Kaspersky. متاح على الرَّابط: https://cutt.us/G5L3h.
3. الشَّامخ، إيمان. خسائر بالملايين... كيف أشعلت فيروسات الفدية النِّيران في عالم التِّقنيَّة؟ مايو 2023م، الجزيرة. متاح على الرَّابط: https://cutt.us/2szL7.
4. العكايلة، عبد الله ماجد عبد المطَّلب. سرقة البيانات والمعلومات الإلكترونيَّة "دراسة مقارنة"، كلِّيَّة العلوم والدِّراسات الإنسانيَّة - قسم القانون، جامعة الأمير سطام بن عبد العزيز. متاح على الرَّابط: https://jfslt.journals.ekb.eg/article_10943_869bcc9f604774fe726ffe0b-c9e5878b.pdf.
5. كيفيَّة حماية الجهاز من البرمجيَّات الخبيثة، salamatechwiki. مُتَاح على الرَّابط: https://cutt.us/ssynj.
6. ما المقصود بالبَرمَجيَّات الضَّارَّة؟ support.google.com. متاح على الرَّابط: https://support.google.com/google-ads/answer/2375413?hl=ar.
7. موصلي، طارق. 7 تهديدات أمنيَّة عند استخدام شبكة الواي فاي العامَّة (وكيف تحمي نفسك منها)، أمن المعلومات، 2021م، متاح على الرَّابط: https://cutt.us/cb7w0.

المراجع الأجنبيَّة:

1. 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe. On Site: https://www.digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-online-safe.
2. Broken cryptography, resources. On site: https://cutt.us/an1BC.
3. Detecting and Responding to Unauthorized Access. Top 8 Practices to Implement, June 28, 2023. On Site: https://www.ekransystem.com/en/blog/detecting-and-responding-to-unauthorized-access.

4. How Ransomware Works, unitrends. On Site: https://www.unitrends.com/solutions/ransomware-education.

5. Kyle Chinj How to Back Up Your Data: 6 Effective Strategies to Prevent Data Loss, 2023. On Site: https://www.upguard.com/blog/how-to-back-up-your-data.

6. Malware, malwarebytes. On Site: https://www.malwarebytes.com/malware.

7. Mitigating malware and ransomware attacks, how to defend organisations against malware or ransomware attacks. On Site: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

8. Mobile Cyber Threats, Kaspersky Lab&Interpol Joint Report. On site: https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf.

9. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088.

10. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088

11. The 12 Most Common Types of Malware, Kurt Baker - February 28, 2023. On Site: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

12. The 5 most common types of data stolen, Lewis Morgan, March 2014. On Site: https://www.itgovernance.co.uk/blog/the-5-most-common-types-of-data-stolen.

13. Top Trends and Threats in Mobile Security: Gartner, cxotoday. On site: https://cutt.us/oMMsw.

14. What do I do to protect against Ransomware? security.berkeley.edu. On Site: https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware.

15. What is data theft and how to prevent it, Kaspersky. On Site: https://www.kaspersky.com/resource-center/threats/data-theft.

16. What Is Network Security? cisco. On site: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

17. What is password protection? Microsoft. On Site: https://www.microsoft.com/en-us/security/business/security-101/what-is-password-protection

18. What is Ransomware? checkpoint. On Site: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

19. What is unauthorized access? nordvpn. On Site: https://nordvpn.com/blog/unauthorized-access/.


CyberEco


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency