تنزيلات البرامج غيـر المُرخّصـة وأضـرارهـا

الفئة المستهدَفة
العمالـة الوافـدة

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

تنزيلات البرامج غير المُرخّصة وأضرارها

الفئة المستهدَفة: العمالة الوافدة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطر

◆ عزيزي المشارك

في ظلّ التطوُّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجِه مختلف شرائح المجتمع، ما يتطلَّب العمل على تعزيز الوعي بمفاهيم السلامة الرقمية؛ التي تُعدّ الدّرع الذي يحمي المجتمع من هذه التهديدات.

وفي سياق جهود «المبادرة الوطنية للسلامة الرقمية» لتعزيز مؤشرات السلامة الرقمية في المجتمع؛ تُقدِّم الوكالة الوطنية للأمن السيبراني هذا الكُتَيِّب، والذي يتضمَّن مجموعةً من النصائح والإرشادات العامَّة المتعلّقة بالسلامة الرقمية.

مُقدّمـــة

يُعدّ "الطفل" Baby هو أول حاسوب رقمي مصمَّم بقدرة برمجة داخلية، تم بناؤه في مانشستر عام 1948م. ويَستخدم جهاز الحاسوب مجموعة من التعليمات التي تُستخدم لتنفيذ مهامّ معيّنة للحصول على نتائج متوقَّعة، ويتضمَّن ذاكرة يتم فيها الاحتفاظ بالبرامج التي تسمح للحاسوب بتنفيذ مهامّ مختلفة بشكل تسلسلي. وقد تم تقديم فكرة تخزين البرامج داخلياً في أواخر الأربعينيات مِن قِبَل عالِم الرياضيات -المجري المولد- جون فون نيومان[1].

ويُجهّز البرنامج من خلال فَهْم طبيعة المهمة أولاً، ثم البدء في إنشاء الكود الخاصّ بها، علماً بأنه يتم إنشاء برنامج الحاسوب من خلال إحدى لغات البرمجة؛ إذ يتم تزويد أجهزة الحاسوب ببرامج متنوّعة مصمَّمة أساساً لمساعدة المستخدِمين على تشغيل المهامّ أو تحسين أداء النظام، وهي لا تقلّ أهميةً عن أجهزة تشغيل نظام الحاسوب. وبهذا فإنّ تنزيل أيّ برنامج حاسوبي من مصدر غير موثوق فيه قد يتسبّب في تصدُّع النظام بأكمله وتعطُّله، وبالتالي الفشل في القيام بالمهامّ الموكلة إليه.

ومع تعدُّد قنوات الحصول على برامج الحاسوب ومجانيّتها؛ قد يلجأ بعض المستخدِمين إلى تنزيلها من على قنوات مجهولة أو غير معتمَدة؛ لهذا يُنْصَح دائماً بتنزيل برامج الحاسوب من مصادرها ويُشتَرط أن تكون مُرخَّصة تجنُّباً للثغرات الأمنية التي قد تقود إلى مهاجمة الحاسوب بالبرمجيات الضّارّة كالفيروسات وبرمجيات التجسُّس... إلى غير ذلك.

1. Computer program. Follow link: https://www.britannica.com/technology/computer-program

01

الفصل الأول

البرامج وقرصنتها

- أولاً: **برامج الحاسوب وأنواعها.**
- ثانياً: **قرصنة البرامج وأنواعها.**
- ثالثاً: **مخاطر تنزيل برامج غير مُرخّصة.**

البرامج وقرصنتها

تُعدّ البرامج الحاسوبية من أهمّ الأدوات في حياتنا اليومية، سواء للاستخدام الشخصي أو المهني؛ حيث تُسهم في تحسين الإنتاجية وتوفير الوقت.

ومع تزايد انتشار التكنولوجيا واعتماد الأفراد والمؤسسات على البرمجيات؛ ظهرت مشكلة قرصنة البرامج، والتي تشمل النَّسخ غير القانوني أو استخدام البرامج دون دَفْع حقوق الملكية.

ولا شك في أن قرصنة البرامج تُشكّل تهديداً للاقتصادات العالمية، وتُؤثّر سلباً على مُطوّري البرامج من خلال تقليص الإيرادات التي تُمكّنهم من الابتكار والتطوير. كما تزيد من مخاطر تعرُّض المستخدمين لهجمات إلكترونية نتيجة تحميل برمجيات غير موثوقة أو مُعدَّلة.

أولاً: برامج الحاسوب وأنواعها

برنامج الحاسوب يُعرف بأنه نظام مكوّن من أمرٍ مُشفّر واحد أو أكثر للقيام بإجراء مُحدَّد على جهاز الحاسوب، وحين تقوم هذه التعليمات بأداء مهمَّة ما مثل تشغيل الجهاز يُطلَق عليها "البرمجيات".

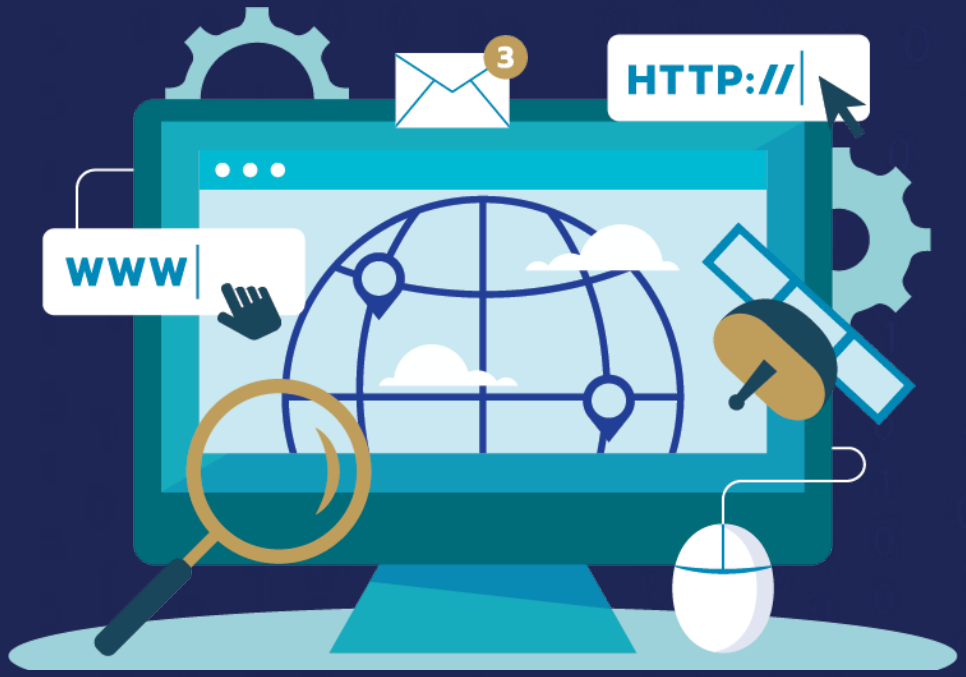
كما يمكن باستخدام التعليمات أداء مهامّ مختلفة، مثل تخزين الملفات، فضلاً عن إنشاء تعليمات لبرنامج ما بواسطة لغة الترميز، التي تُحَوِّل الأوامر إلى أحد أشكال التعليمات البرمجية؛ ليتمكّن الحاسوب من استيعابها وتنفيذ ما بها.

هل تعلم؟

نظراً للتهديد المترتب على البرامج غير المُرخَّصة، أصدرت مايكروسوفت Microsoft أكثر من 50 نشرة أمان تتعلق بنظام Windows منذ عام 2003م؛ لخطورة تسلُّل المهاجمين إلى جهاز الحاسوب الخاص بالمستخدمين عبر نقاط الضعف في نظام التشغيل[1].

1. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

ومن أهم أنواع البرامج التطبيقية:



متصفّح الإنترنت (Internet Browser)

هو برنامج يُستخدَم للوصول إلى صفحات الويب المختلفة، مثل مواقع البحث أو المواقع الإلكترونية. لا يقوم المتصفّح بنفسه بعَرْض نتائج البحث، بل يعتمد على محركات البحث (مثل Google) للبحث عن المعلومات المطلوبة. ومن خلال كتابة عنوان موقع أو كلمات مفتاحية في شريط العنوان أو البحث، يتم توجيه المستخدِم إلى نتائج ذات صلة من خلال مُحرّك البحث[1].

1. Ecommerce fraud trends and statistics merchants need to know in 2024, Mastercard, on site: https://2u.pw/v02pFMa9

يتميّز المتصفّح بإمكانية عرض النصوص، الصور، الفيديوهات، وغيرها من المحتويات من جميع أنحاء العالم. كما أن الروابط التشعبية (Hyperlinks) داخل صفحات الويب تُمكّن المستخدِم من التنقُّل بين الصفحات المختلفة. كلّ صفحة ويب أو ملف تحتوي على عنوان URL (محدد موقع الموارد)، وهو ما يساعد المتصفح في تحديد موقع المحتوى المطلوب، وعرضه على المستخدِم.

هل تعلم؟

تقوم ملفات تعريف الارتباط (Cookies) بتخزين بيانات معينة حول المستخدِم، مثل تفضيلاته أو معلومات تسجيل دخوله، على جهازه؛ وذلك لتسريع تجربته عند زيارة نفس المواقع في المستقبل. بعض ملفات تعريف الارتباط قد تقوم بتخزين معلومات تفصيلية حول اهتمامات المستخدِم لعرض إعلانات مُوجَّهة إليه. أما ملفات تعريف الارتباط الخاصة بالطرف الثالث (Third-party Cookies)؛ فهي تجمع بيانات حول المستخدِم عبر مواقع متعدّدة، وتُستخدَم لأغراض تسويقية. وبعض المتصفّحات تُتيح إمكانية حَظْر هذا النوع من الملفات[1].

هل تعلم؟

على الرغم من أن معظم المتصفحات تدعم وضع التصفُّح الخاص (مثل وضع "التخفّي" Incognito Mode)، فإن هذا الوضع لا يُخفي هوية المستخدِم أو بيانات التصفُّح عن مزوّدي خدمات الإنترنت أو الحكومات. ما يقوم به هذا الوضع هو عدم حفظ سِجِلّ التَّصفُّح وكلمات المرور على الجهاز نفسه، ممّا يجعله مفيداً عند استخدام أجهزة عامة.

1. What are Cookies?. Follow link: https://www.kaspersky.com/resource-center/definitions/cookies

مُعالِج النصوص (Word Processor)

معالج النصوص هو برنامج يُستخدَم لإدخال النصوص وتحريرها وتنسيقها؛ يسمح بتغيير مظهر النصوص، مثل تغيير حجم الخطوط أو ترتيب الفقرات، ويُتيح إضافة عناصر مرئية مثل الجداول أو الرسوم البيانية. يمكن أيضاً التحكُّم في حقوق التحرير عند مشاركة المستند مع الآخرين.

تتضمَّن معظم برامج معالجة النصوص أدوات لتدقيق النصوص إملائياً ونحوياً، وتوفّر بعض البرامج قاموساً للمرادفات لمساعدة المستخدِم في تحسين جودة الكتابة.

برامج عقد المؤتمرات عن بُعْد (Teleconferencing Software)

هذه البرامج تَسْمح بالتواصل الصوتي والمرئي بين المستخدِمين عن بُعْد، وهي تُستخدَم بكثرة في الاجتماعات المهنية، خاصةً مع انتشار العمل اللامركزي. وتُتيح مشاركة الحاضرين في اجتماعات فيديو أو صوت، كما تختلف جودة وعدد المشاركين المسموح بهم بناءً على البرنامج المستخدَم.

هذه البرامج أصبحت ضرورية لتقليل التكاليف المالية المرتبطة بالاجتماعات التقليدية واستئجار المكاتب[1].

1. What Is Video Conferencing Software?. Follow link: https://www.bigcommerce.com/glossary/video-conferencing-software/

جداول البيانات الرقمية (Digital Spreadsheets)

جداول البيانات الرقمية مثل Microsoft Excel هي أدوات فعَّالة لتخزين البيانات وتنظيمها في شكل جداول وصفوف. تُتيح للمستخدِمين إجراء عمليات حسابية متقدّمة وتصنيف البيانات بشكل يُسهّل قراءتها وتحليلها[1].

تُوفّر هذه البرامج القدرة على استيراد البيانات الخارجية وإدخالها بسهولة، وتعديل القوالب المختلفة وفقاً لاحتياجات المستخدِمين، إضافةً إلى مشاركة المستندات مع الزملاء.

أدوات إدارة المشاريع (Project Management Tools)

هذه التطبيقات تُستخدَم لتنظيم وتخطيط المهامّ في بيئات العمل التعاونية. وتُوفّر ميزات لتوزيع المهامّ بين الفريق، وتتبُّع التقدُّم، وضَبْط المواعيد النهائية للمشاريع[2]. وتساعد هذه الأدوات الإداريين على مُراقبة تقدُّم العمل وتوزيع الأعباء بين الموظفين بكفاءة، مما يُسهم في تحسين الإنتاجية وتقليل الوقت الضائع.

1. Katie Terrell Hanna, spreadsheet. Follow link: https://www.techtarget.com/whatis/definition/spreadsheet
2. Deepak Palasamudram, What is Project Management?, Dec 2022. Follow link: https://2u.pw/RYVwfkV4

ثانياً: قرصنة البرامج وأنواعها

يُقصَد بها الاستخدام غير القانونيّ وغير الأخلاقي لبرامج الحاسوب المصرَّح بها، مثل القيام بنَسْخها أو سرقتها أو توزيعها أو تعديلها أو نَقْلها بطرق غير قانونية. ويدخل في هذا التعريف مشاركة أيّ شخص في تنفيذ هذا؛ سواءٌ أكان بقَصْد أم لا؛ حيث يكفي استخدام برامج بطرق غير قانونية أو نسخ وتوزيع برامج مُرخّصة دون إذن المالك[1].

احذر!

تشمل عملية قرصنة برامج الحاسوب بشكل غير قانوني: نَسْخ البرامج أو سرقتها، أو مشاركتها مع الآخرين؛ أو استخدام تلك البرامج بصورة غير قانونية دون إذن المالك.

هل تعلم؟

في يونيو 2018م، كشفت أبحاث عملية أن 37% من البرامج التي جرى تنزيلها على أجهزة الحاسوب سواء المكتبية أو المحمولة غير مصرَّح بها.

1. What is Software Piracy?. Follow link: https://www.javatpoint.com/what-is-software-piracy

أنواع قرصنة البرامج

سرقة البرامج أو قرصنة المستخدِم النهائي SOFTLIFTING OR END-USER PIRACY

تتم قرصنة البرامج عند شراء إصدار واحد من البرنامج، ثم تنزيله لاحقاً على العديد من الأجهزة، والسبب وراء ذلك إما توفير المال وإما كَسْب المال؛ وذلك يُعدّ مخالفاً للقوانين.

تجاوز الترخيص LICENCE OVERUSE

يحدث ذلك عند استخدام عدد كبير من المستخدِمين على نفس الشبكة نُسخة أصلية من البرنامج في الوقت نفسه، أو وصول العديد من المستخدِمين إلى البرنامج؛ رغم قَصْر استخدامه على عدد مُحدَّد.

التزوير COUNTERFEITING

التزوير أو التقليد هو نسخ البرامج ونشرها بصورة غير قانونية، ثم بيع هذه النُّسَخ بسعر أقل من السعر الحقيقي للبرنامج الأصلي [1].

1. Software Piracy Facts. Follow link: https://hypertecsp.com/knowledge-base/software-piracy-facts/

القرصنة عبر الإنترنت ONLINE PIRACY

يُطلَق هذا الاسم على حالات الحصول على برامج بصورة غير قانونية، ومِن ثَم نشرها عبر الإنترنت، فغالباً ما تُتيح شبكات مشاركة الملفات من نظير إلى نظير للمستخدِمين حِفْظ ومشاركة البرامج الأصلية المحمية بحقوق الطبع والنشر.

تحميل القرص الصلب HARD DISK LOADING

هذا النوع يعتمد على قيام شخصٍ ما بنَسْخ البرنامج بعد شرائه بصورة طبيعية، ثم تحميله على القرص الصلب بجهاز الحاسوب، ثم القيام ببيع هذا الجهاز.

احذر!

نسخ البرنامج الحاسوبي بصورة طبيعية، وتحميله على القرص الصلب بجهاز الحاسوب، ثم القيام ببيع الجهاز بعد ذلك، يُعدّ شكلاً من أشكال قرصنة البرامج.

معلومة

في عام 2012م، أكَّدت دراسة أن 97% من إجمالي الموادّ المُنتَجة في بيئة الأعمال تُخزَّن رقمياً، وهذه البيانات تبلغ ما يُقدَّر بـ1,7 تريليون دولار سنوياً، ممَّا يترتَّب عليه خسائر باهظة في حال وقوعها في أيدي مجرمي الإنترنت.

دوافع تنزيل برامج غير مُرخَّصة

التكلفة المالية:

عادةً ما تكون البرامج غير المُرخّصة مجانية، أو أرخص من البرامج الأصلية، وهو يُعدّ سبباً رئيساً وراء سعي بعض الأفراد بل والشركات لتنزيلها؛ توفيراً للنفقات.

التوافر:

بعض البرامج لا تُوجَد في متاجر التطبيقات؛ مما يدفع البعض للبحث عنها في مصادر أخرى غير موثوقة.

الوظائف الإضافية:

تحتوي البرامج غير المُرخَّصة على ميزات ووظائف إضافية لا توجد في البرامج الأصلية، ممَّا يجعلها أكثر جذباً للأفراد.

سهولة التنزيل:

يلجأ بعض الأفراد لتنزيل البرامج غير المُرخّصة لسهولة تنزيلها، بخلاف البرامج الأصلية التي تتطلَّب عملية تحقُّق قبل التنزيل.

احذر!

وفقاً لمسح البرامج العالمي لعام 2018م، فإن 37% من البرامج المثبَّتة على أجهزة الحاسوب الشخصية هي برامج غير مُرخّصة.

هل تعلم؟

ما يتم نَسْخه من برامج حاسوبية ونَشْره بصورة غير قانونية يُعدّ أحد أوجه قرصنة البرامج، ويُطلَق عليه التزوير أو التقليد، وغالباً ما يتم بيع هذه النُّسَخ بسعر أقل من السعر الحقيقي للبرنامج الأصلي.

ثالثاً: مخاطر تنزيل برامج غير مُرخّصة

أصبحت التَّهديدات السيبرانية في تزايدٍ واضح، فمع الاعتماد على الأجهزة الإلكترونية في أداء الكثير من المهامّ اليومية والعملية؛ فإنها تتعرَّض باستمرار للفيروسات والبرمجيات الضّارَّة التي تؤدّي إلى اختراق المعلومات الحساسة، والخسارة المالية، وحتى سرقة الهوية. وتختلف الأضرار ما بين الأفراد والشركات، وهي كالتالي:

على مستوى الأفراد

الإصابة بالبرمجيات الضّارَّة

يزيد تثبيت برامج غير مُرخّصة على أجهزة الحاسوب من فرص مواجهة برمجيات ضارَّة، على سبيل المثال، في عام 2017م، تسبَّب هجوم واسع النطاق للبرمجيات الضّارَّة المعروفة باسم WannaCry في إصابة أكثر من 300,000 جهاز حاسوب في جميع أنحاء العالم من خلال تنزيل ضارّ[1].

وتعمل البرامج غير المُرخّصة (المقرصنة) أيضاً على تعزيز انتشار أحصنة طروادة والروبوتات؛ إذ تتنكر أحصنة طروادة في شكل برامج حميدة لكنّها في الواقع تسمح للمهاجم بالتحكم عن بُعد في نظام المستخدِم الضحية. كما تسمح الروبوتات للمهاجم بالتحكُّم في الأجهزة المصابة لتنفيذ وظائف غير قانونية دون عِلْم المستخدِم[2].

وكذلك يرتبط بالبرامج غير المُرخّصة نشر برمجيات الفدية؛ ممَّا يتسبّب في تعطُّل ملفات المستخدمين وتشفيرها مقابل دفع المال، وفي حال عدم الدفع يقوم المهاجم الإلكتروني إما بتدمير مفتاح التشفير وإما بنشر الملفات المسروقة على الإنترنت.

1. Investigation: WannaCry cyber attack and the NHS 27 October 2017 https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs
2. What is Pirated Software?. Follow link: https://cyberpedia.reasonlabs.com/EN/pirated%20software.html

احذر!

تسمح الروبوتات للمهاجم بالتحكُّم في الأجهزة المصابة لتنفيذ وظائف غير قانونية دون علم المستخدم، والسبب وراء ذلك تثبيت البرامج غير المُرخّصة.

فقدان البيانات الشخصية

يؤدي التنزيل من مصادر غير موثوقة إلى تعريض البيانات الحساسة للخطر؛ إذ يمكن للمتسللين استخدام أساليب مختلفة، مثل التصيد الاحتيالي وتسجيل لوحة المفاتيح، لسرقة البيانات الشخصية والمالية للمستخدمين مما يؤدي إلى سرقة الهوية والاحتيال المالي وعواقب خطيرة أخرى. ففي عام 2018م، اختُرِقَت المعلومات الشخصية لملايين من مستخدمي فيسبوك؛ بسبب اختراق البيانات الناتج عن تطبيق تابع لجهة خارجية.

مخاطر برمجيات التجسُّس

تزوّد البرامج غير المُرخّصة المهاجمين الإلكترونيين بثغرات يمكنها من خلالها التسلل إلى الشبكة الخاصة بالمستخدمين أو الشركات؛ ما يترتب عليه تدمير البيانات وانتهاك الخصوصية.

وبرمجيات التجسس هي نوع من البرمجيات الضّارّة التي تراقب أنشطة جهاز الحاسوب سراً تمهيداً لسرقة معلومات المستخدم الشخصية، بما في ذلك كلمات المرور وتفاصيل بطاقات الائتمان، ويؤدّي تنزيل برامج غير مُرخّصة إلى فتح الباب أمام برمجيات التجسُّس.

عدم استقرار النظام

عدم تلقّي المستخدِم إشعارات أو مساعدة من الشركة المنتجة للبرنامج بشكل قانوني؛ يشير إلى ارتفاع احتمالية تعطُّل البرنامج غير المُرخّص؛ نتيجة افتقار البرامج غير المُرخّصة إلى التصحيحات والتحديثات التي تَتِمّ على البرامج الأصلية[1]؛ مما يتسبَّب في عدم استقرار جهاز الحاسوب، وحدوث أعطال متكررة وفقدان البيانات، إلى جانب استغراق وقت طويل في إصلاح الأعطال، وبالتالي التأثير سلباً على إنتاجية المستخدِم في حال استخدام هذه البرامج في عمله.

احذر!

يؤدي عدم تلقّي المستخدم إشعارات أو مساعدة من الشركة المُنتِجة للبرنامج -لكونه ثُبِّت بشكلٍ غير قانونيّ- إلى ارتفاع احتمالية تعطُّل البرنامج غير المُرخّص، نتيجة افتقار البرامج غير المُرخّصة إلى التصحيحات والتحديثات التي تَحْدث في البرامج الأصلية.

العواقب القانونية

تُعدّ قرصنة البرامج جريمة يعاقب عليها القانون، بموجب قوانين حقوق الطبع والنشر التي تهدف إلى الحفاظ على مصالح مُطوّريها. مما يؤدي إلى غرامات باهظة أو اتهامات جنائية.

1. Devin Partida, Why You Shouldn't Use Pirated Software (But Why People Still Do), 2020. Follow link: https://www.computer.org/publications/tech-news/trends/why-you-shouldnt-use-pirated-software

مشكلات عدم التوافق

لا تخضع البرامج غير المُرخّصة للاختبارات الضرورية لضمان التوافق مع أجهزة وبرامج الحاسوب، وهذا يتسبَّب في ما يُعرَف بمشكلات التوافق، ومِن ثَم تعطُّل الحاسوب أو فشله في أداء المهام بشكلٍ صحيح[1].

الخسائر المالية

رغم مجانية البرامج غير المُرخّصة؛ إلا أنها تُكلِّف المستخدِم مالاً أيضاً، والذي يأتي في صورة إعلانات منبثقة أو غير مرغوب فيها، أو مطالبات مالية مقابل الحصول على الوظائف الكاملة، أو حتى تسجيل المستخدِم في اشتراكات مدفوعة دون مُوافقته.

تحديثات الأمان المخترقة

قد يحدث تداخل بين البرامج غير المُرخّصة وتحديثات أمان الحاسوب، مما يجعل نظامه عُرضَة لتهديدات سيبرانية جديدة، وهذا يُعدّ أمراً خطيراً نتيجة تطوير مجرمي الإنترنت لأساليب جديدة دائماً لاستغلال الثغرات الأمنية في البرامج المعروفة.

1. Don't Risk It: The Top 10 Dangers of Downloading Unverified Software, March 2023. Follow link: https://www.lockwell.co/blog/don-t-risk-it-the-top-10-dangers-of-downloading-unverified-software

احذر!

لا تَخْضع البرامج غير المُرخّصة للاختبارات الضرورية لضمان التوافق مع أجهزة وبرامج الحاسوب، وهذا يتسبّب في ما يُعرَف بمشكلات التوافق، ومِن ثَم تعطُّل الحاسوب أو فشله في أداء المهام بشكلٍ صحيح.

هل تعلم؟

يُكلّف هجوم البرمجيات الخبيثة ما متوسطه 2.4 مليون دولار للشركة الواحدة، ويحتاج نحو 50 يوماً للانتهاء.

على مستوى الشركات

مخاطر خصوصية البيانات

يؤدّي قيام الموظفين بشراء واستخدام برامج الطرف الثالث، دون عِلْم قسم تكنولوجيا المعلومات في الشركات، إلى تعريض البيانات الحساسة للخطر؛ حيث يتسبَّب التحكم اللامركزي في أصول البرامج في منع فريق تكنولوجيا المعلومات من تطوير وتنفيذ الخطوات اللازمة للحد من المخاطر؛ نظراً لأن مثل هذه البرامج غير المصرَّح بها خارج سيطرتهم.

مخاطر الامتثال

نظراً لأن البرامج تخضع لحقوق الملكية الفكرية، فإن استخدام غير المصرح به منها؛ يؤدي بالشركات إلى دفع الغرامات، والتعرض للعقوبات القانونية، إلى جانب فقدان البيانات الحساسة؛ نتيجة الثغرات الأمنية الخطيرة بهذه البرامج التي لا تخضع للتصحيحات كغيرها من البرامج الأصلية.

02

الفصل الثاني

مخاطر البرامج غير المُرخّصة

- أولاً: الفيروسات الأكثر شيوعاً المرتبطة بالبرامج غير المُرخّصة.
- ثانياً: العلامات التحذيرية من البرامج غير المُرخّصة.
- ثالثاً: الحماية من البرامج غير المُرخّصة.

مخاطر البرامج غير المُرخّصة

تُعدّ البرامج غير المُرخّصة مصدراً رئيساً للمخاطر الأمنية والاقتصادية في العصر الرقمي؛ حيث يلجأ بعض الأفراد إلى استخدام هذه البرامج لتجنُّب تكاليف التراخيص، لكنَّهم يَغفلون عن التهديدات الخفية التي تحملها؛ فالبرامج غير المُرخّصة غالباً ما تكون مُعدَّلة أو مُخترَقة، مما يجعلها عُرضة للبرمجيات الخبيثة والفيروسات التي قد تؤدي إلى اختراق الأنظمة وسرقة البيانات الحساسة. وبالإضافة إلى المخاطر الأمنية؛ يمكن أن يُواجِه المستخدمون مشكلات قانونية وعقوبات مالية بسبب انتهاك حقوق الملكية الفكرية، واستخدام البرامج المُرخّصة يضمن الحماية والأداء الأمثل، ويحافظ على الأمن الرقمي والالتزام بالقوانين.

أولاً: الفيروسات الأكثر شيوعاً المرتبطة بالبرامج غير المُرخّصة

تُعدّ الفيروسات المرتبطة بالبرامج غير المُرخّصة أحد أخطر التهديدات الأمنية في عالم التكنولوجيا اليوم. وتعتمد هذه الفيروسات على استغلال نقاط الضعف التي تنشأ عندما يقوم المستخدمون بتحميل برامج غير مُرخّصة أو مُقلّدة من مصادر غير موثوقة. وغالباً ما تحتوي هذه البرامج على برمجيات ضارّة تُدمَج فيها مِن قِبَل مجرمي الإنترنت الذين يستغلون حاجة الأفراد للحصول على البرامج مجاناً أو بتكلفة أقلّ من الشرعية.

ومن أشهر أنواع الفيروسات التي ترتبط بالبرامج غير المُرخّصة ما يلي:

دودة كونفيكر Conficker

هي دودة حاسوبية تستهدف نظام التشغيل مايكروسوفت ويندوز Microsoft Windows، وقد تم اكتشافها لأول مرة في نوفمبر 2008م؛ حيث تَستخدم الثغرات الأمنية في برامج نظام التشغيل "ويندوز" لتنفيذ هجمات القاموس على كلمات المرور، وكان يصعب مكافحتها بسبب استخدامها للعديد من تقنيات البرمجيات الضّارَّة المتطورة[1].

تتميز الدودة الحاسوبية بسرعة انتشارها، وقُدرتها على تعطيل ميزات الأمان، وإيقاف إعدادات النسخ الاحتياطي التلقائي، بالإضافة إلى حذف نقاط الاستعادة، وفتح قنوات اتصال لتلقي الأوامر من جهاز حاسوب بعيد. وبمجرد إصابة الجهاز الأول، تبدأ بالانتشار عبر الشبكة بأكملها من خلال نَسْخ نفسها إلى المجلدات المشتركة.

أحد الأسباب الرئيسة لانتشار هذا النوع من البرمجيات الضّارَّة هو استخدام البرامج غير المُرخّصة أو المزيَّفة. وتُعدّ دودة Conficker -التي انتشرت على مستوى العالم بين عامي 2008 و2009م- مثالاً بارزاً على ذلك. وقد حذَّر خبراء الأمن السيبراني حينها من خطورة تحميل البرامج غير المُرخّصة، التي تُعدّ من أكثر الطرق شيوعاً للإصابة بهذه الدودة.

انتبه!

يتم إنتاج ما لا يقل عن 500.000 نوع جديد من البرمجيات الضّارَّة يومياً[2].

1. Lital Asher-Dotan, What is the Conficker worm. Follow link: https://www.cybereason.com/blog/what-is-the-conficker-worm
2. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

هل تعلم؟

أكّدت دراسة استقصائية أجرتها جامعة سنغافورة الوطنية حول عمليات شراء أجهزة الحاسوب المُجمَّعة في 11 دولة حول العالم -والتي يتمّ تثبيت برامج غير مُرخّصة عليها- أن:

- 61% من الأجهزة كانت مصابة بالبرمجيات الضّارّة.
- 24% من البرمجيات الضّارّة المجمَّعة مع تنزيلات البرامج غير المُرخّصة تسبَّبت في إلغاء تنشيط برامج مكافحة الفيروسات على أجهزة الحاسوب.
- نحو 31% من البرامج غير المقرصنة التي لم تكتمل عملية تثبيتها أعادت توجيه حركة المرور إلى مواقع تُعرِّض المستخدمين للبرمجيات الضّارّة والإعلانات غير المرغوب فيها[1].

1. Raja Viswanathan, Remote work, pirated software, and local admin rights: A deadly cocktail. Follow link: https://www.securden.com/blog/pirated-software-malware.html

ثانياً: العلامات التحذيرية من البرامج غير المُرخّصة

- ظهور عرض لفحص النظام على شاشة الحاسوب، فهنا ينبغي الحذر من الإعلانات المنبثقة للبرامج؛ فإذا ظهر إعلان ما -والذي عادةً يتخفَّى في هيئة "تحذير أو تنبيه"- على الشاشة ويطلب فحص الحاسوب بحثاً عن البرمجيات الضّارَّة؛ فلا يجب الضغط عليه.

  فالعديد من النوافذ المنبثقة المزيفة تقوم بتثبيت برنامج تسجيل ضغطات المفاتيح، لسرقة بيانات الدخول الخاصة بالمستخدِم؛ لذا يُنْصَح بشراء برنامج مكافحة الفيروسات والبرمجيات الضّارَّة من مواقع ذات سُمعة متميزة[1].

- تلقّي تحذيرات من امتلاء الحاسوب بالفيروسات؛ فهذه التحذيرات قد تكون مزيفة؛ حيث تَعرض مقترحاً لتثبيت برنامج لتنظيف جهاز الحاسوب، لكنَّ الأمر قد يتخطَّى ذلك إلى حد إصابته بالبرمجيات الضّارَّة.

- طلب المعلومات الشخصية: عادة ما تتمّ عمليات الاحتيال من خلال بريد إلكتروني مُصَاب يُوفِّر طريقة لتثبيت البرمجيات الضّارَّة على النظام، وهنا يؤدّي البرنامج غير المُرخّص إلى تلقّي المستخدِم تنبيهاً يُشبه تنبيهات برامج مكافحة الفيروسات، وعند الضغط عليه سيطلب منه معلومات شخصية، مثل رقم البطاقة الائتمانية، وغيرها.

1. Do You Know How To Spot Fake Software And Updates? Learn The 7 Red Flags!. Follow link: https://www.alvareztg.com/do-you-know-how-to-spot-fake-software-and-updates-learn-the-7-red-flags/

- ظهور نافذة منبثقة تطلب تحديثاً إضافياً؛ عند تصفُّح الويب قد تظهر نافذة منبثقة تزعم أن برنامجاً ما بحاجة للتحديث، أو هناك صعوبة في عرض الصفحة، وفي حقيقة الأمر هذه النوافذ خادعة؛ فهي برمجيات ضارَّة بمجرد الاستجابة لما يظهر، يتم تنزيلها إلى الجهاز.
- تلقّي تحذيرات من برنامج لم تقم بتنزيله؛ بعض المستخدمين لا يفحصون البرامج على أجهزتهم بانتظام؛ مما يجعلهم عُرضة للوقوع في فخّ الخداع والضغط على الرسالة التحذيرية المُزيَّفة قبل التأكُّد من تثبيت البرنامج بالفعل على الجهاز، وهذا منتشر على أجهزة الحاسوب الشخصية.
- تلقي تحذيرات في صورة رسائل منبثقة، تفيد بأن المتصفّح قديم، وهي إحدى العلامات على تنزيل برامج غير مُرخّصة، والتي قد تتسبَّب في دخول المستخدِم الضحية إلى مواقع ويب مُزيَّفة تسرق بياناته الشخصية.
- غياب التحديثات أو دعم العملاء بالبرنامج غير المُرخّص، بخلاف المعتاد في البرنامج الأصلي الذي يُوفِّر تحديثات تلقائية ودعماً للعملاء.
- العروض المخادعة، ينبغي الحذر الشديد من العروض التي توفّر برامج باهظة الثمن مجاناً، فهي عادة ما تكون برامج غير مُرخّصة تَضُرّ الأجهزة[1].

1. Clare Stouffer, Are you accidentally pirating software? ,January 2024. Follow link: https://us.norton.com/blog/malware/accidentally-pirating-software

ثالثاً: الحماية من البرامج غير المُرخّصة

- الالتزام بالمصادر الموثوقة عند تنزيل البرامج؛ مثل: متاجر التطبيقات الرسمية كجوجل بلاي Google Play، فهي لديها إجراءات أمنية تُقلّل من مخاطر البرمجيات الضّارّة والتهديدات السيبرانية.
- الحذر من الضغط على الإعلانات المنبثقة أو الروابط المجهولة؛ لأنها قد تؤدي إلى إعلانات غير موثوقة.
- استخدام برامج مكافحة الفيروسات الموثوقة، مع الحرص على تحديثها لاكتشاف البرمجيات الضّارّة وإزالتها من جهاز الحاسوب.
- الحذر من التنزيلات المجانية التي غالباً ما تَجْذب الأفراد لعدم تحمُّلهم تكاليف مالية عند تنزيلها، بل يجب البحث عن المصدر الموثوق فيه، وقراءة المراجعات قبل التنزيل.
- استخدام شبكة افتراضية خاصة (VPN)؛ لتوفير طبقة أمان إضافية؛ من خلال تشفير الاتصال بالإنترنت، وإخفاء عنوان IP الخاص بالمستخدِم، ممَّا يُصعِّب مهمة وصول مجرمي الإنترنت إلى أجهزة المستخدِمين.
- الامتثال لممارسات الأمن السيبراني من حيث الحفاظ على تحديث البرامج والأنظمة، وتأمينها وتصحيحها بانتظام من الثغرات الأمنية، والتدريب على تحديد الأنشطة المشبوهة يساعد إلى جانب برامج مكافحة الفيروسات في تعزيز الحماية.

كيف يمكن التأكُّد من سلامة عملية تنزيل البرامج؟

◆ التحقق من شرعية موقع الويب

في حال تنزيل برنامج أو تطبيق من الإنترنت؛ ينبغي التأكد أولاً من حُسْن سمعة الموقع، فمثلاً في حال تنزيل برنامج من شركة البرمجيات المعروفة مايكروسوفت Microsoft؛ فهذا يعني أن الموقع آمِن، لكن هذا قد لا ينطبق على باقي مواقع الويب، ويُفضَّل دائماً عند الرغبة في تنزيل برنامج تم إنشاؤه بواسطة Microsoft أن يتم ذلك من الموقع الرسمي.

وبصفة عامة، للتحقُّق من شرعية موقع ويب ما، هناك طريقتان هما:

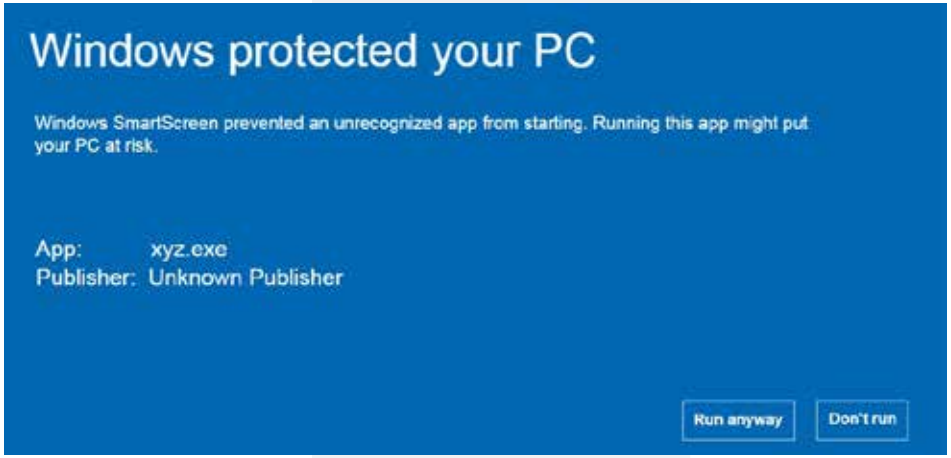
- **التحقق من تفاصيل شهادة SSL/TLS**، فإذا رأيت رمز قفل الأمان أو "HTTPS" في شريط العناوين قبل عنوان URL لموقع الويب، فهذا يعني أنه آمِن. بالطبع هذا إلى جانب هوية الجهة المطلقة للموقع مثل مايكروسوفت مثلاً، وليس جهة مجهولة[1].

صورة توضيحية لعلامات الأمان في موقع الويب الشرعي

1. How to check if a file is safe to download. FOLLOW LINK: https://www.microsoft.com/en-us/edge/learning-center/how-to-check-if-a-file-is-safe-to-download?form=MA13I2

- **التحقق من النوافذ المنبثقة لـ Windows Defender SmartScreen**، فهي تُعدّ ميزة أمان مُهمَّة للتحقُّق تلقائياً من التنزيلات الخطيرة، ويُفضَّل تفعيلها على جهاز الحاسوب سواء الشخصي أو المحمول الذي يعمل بنظام ويندوز. فعلى سبيل المثال عند محاولة تنزيل برنامج من جهة غير معروفة بواسطة متصفح Microsoft Edge أو أيّ مُتصفّح آخر ستظهر رسالة تحذيرية من احتمالية تعرُّض الجهاز للتلف أو سرقة البيانات.

أما إذا وقَّع أحد مُطوّري البرامج التعليمات البرمجية الخاصَّة به بواسطة شهادة توقيع رمز التحقق الموسَّع، فعندها يتم الوثوق به تلقائياً بواسطة Microsoft، ولن تظهر الرسائل التحذيرية[1].



صورة توضيحية لعلامات الأمان في موقع الويب الشرعي

1. Microsoft Defender SmartScreen. FOLLOW LINK: https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

◆ التحقُّق من حجم الملف وامتداده

إذا كان حجم الملف المراد تنزيله من الإنترنت أصغر أو أكبر من المتعارَف عليه؛ فهذا يعني أنه ليس آمِناً. فغالباً يقوم مجرمو الإنترنت بإنشاء ملفات متشابهة مع البرامج المشروعة؛ لخداع المستخدمين لتنزيلها.

وكذلك التحقق من امتداد جميع الملفات للتأكُّد من صحتها؛ ففي حال تنزيل مستند وورد Word فلا ينبغي تصنيفه كملف قابل للتنفيذ exe[1].

◆ التحقُّق من مراجعات مستخدِمي البرنامج

مراجعة تجارب المستخدِمين حول البرنامج قبل التنزيل؛ تساعد في تفادي مشكلات كثيرة من البداية. ولهذا فقبل تنزيل أيّ تطبيق للجوال من Ap-ple App Store أو Google PlayStore ينبغي التحقُّق من المراجعات قبل تنزيله، وإذا كانت التقييمات غير جيدة فلا يُحبَّذ تنزيله.

◆ استخدام برامج فحص الفيروسات للتحقُّق من التنزيلات بحثاً عن البرمجيات الضّارَّة

تساعد هذه البرامج في اكتشاف الفيروسات والأنواع المختلفة من البرمجيات الضّارَّة وإزالتها، ولهذا إذا كان المستخدِم على وشك تنزيل ملف قابل للتنفيذ مثل "exe" فعليه التيقظ لأنّ أيَّ برمجية ضارة على الملف ستُصيب نظام الحاسوب وتُهدّد بياناته بالسرقة.

1. How Can I Tell If a Download Is Safe?. FOLLOW LINK: https://codesigningstore.com/how-to-tell-a-download-is-safe

◆ الحذر أثناء تنزيل وفتح مرفقات البريد الإلكتروني

يؤدي تنزيل مرفق مُصاب أو ضارّ مرسَل عبر البريد الإلكتروني من جهات غير معروفة، إلى إصابة الأجهزة والنظام بالكامل، وتعريض البيانات لمخاطر جمَّة، ويستخدم مجرمو الإنترنت أنواعاً معينة من الملفات مثل ملفات exe، والملفات المضغوطة، ومستندات Office؛ لنشر البرمجيات الضّارَّة تمهيداً لتنفيذ هجومهم، ولتفادي ذلك يجب الامتناع عن تنزيل مرفقات من جهات اتصال مجهولة.

معلومة

أكثر من 90% من البرمجيات الضّارَّة تنتشر عبر رسائل البريد الإلكتروني، وذلك وفقاً لبيانات من تقرير التحقيقات في خرق البيانات لعام 2018م (DBIR) الصادر عن شركة Verizon.

التمارين تعتمد على المادة العلمية المقدَّمة في سياق هذا الكتيب، وهي مذكورة هنا بدون حل، وتم إرفاق الحل في نهاية الكُتَيِّب.

التمرين الأول

• اختر الإجابة الصحيحة

1. يمكن استخدام برامج الحاسوب في أداء وظائف مختلفة، منها .....

1. البحث عن المعلومات عبر شبكة الإنترنت.
2. تصنيف وتخزين البيانات على الحاسوب.
3. توفير الحماية للحاسوب من البرمجيات الخبيثة مثل الفيروسات.
4. جميع ما سبق.

2. تقوم ملفات تعريف الارتباط Cookies بـ .....

1. بيع معلومات المستخدمين إلى أطراف خارجية.
2. تفعيل وضع المتصفح الخفي على المتصفحات الرئيسية.
3. حفظ المعلومات الخاصة بالمستخدم على جهاز الحاسوب الخاص به؛ لاستخدامها مجدداً في حال زيارة مواقع الويب.

3. من أنواع قرصنة البرامج .....

1 أحصنة طروادة.

2 تحميل القرص الصلب.

3 الفيروسات.

4. ..... هو ما يتم نسخه من برامج ونشره بصورة غير قانونية بغرض التقليد، وغالباً ما يتم بيع هذه النُّسَخ بسعر أقل من السعر الحقيقي للبرنامج الأصلي.

1 القرصنة عبر الإنترنت.

2 تحميل القرص الصلب.

3 التزوير أو التقليد.

5. من أسباب تنزيل برامج غير مُرخّصة .....

1 التكلفة المالية المنخفضة والتساهل في إجراءات التثبيت.

2 صعوبة التنزيل قبل التحقق.

3 تضمنها ميزات ووظائف إضافية.

التمرين الثاني

اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخاطئة، مع تصويب الخطأ:

1. لا ترتبط "ملفات تعريف الارتباط الخاصة بالطرف الثالث third-party cookies" بما يزوره المستخدم من مواقع ويب، بل تتبع المستخدم عبر المواقع لجمع المعلومات عنه وبيعها لجهات خارجية.

2. بعض ملفات تعريف الارتباط تحتفظ بمعلومات أكثر دقة، مثل اهتمامات المستخدم لتوجيهه إلى محتويات متوافقة معها.

3. من الاعتقادات الصحيحة أن "وضع التصفح المتخفي incognito mode" يخفي هوية المستخدِم وسجل التصفُّح عن مزودي خدمات الإنترنت والحكومات والمعلنين.

4. يساعد معالج النصوص Word processor في حال الرغبة في مشاركة مستند ما مع آخرين، في وضع حدود لتدخلاتهم في تحرير محتوى المستند.

5. تصعب جداول البيانات الرقمية على المستخدمين مسألة تصنيف البيانات في أعمدة وصفوف وأقسام واضحة تسهل قراءتها وفهمها.

6. بواسطة جداول البيانات الرقمية يمكن جدولة واجبات العمل ووضع الأنشطة الحالية أو المخططة للجميع في بيئة العمل على لوحة رقمية واحدة.

7. يدخل في قرصنة البرامج: مشاركة أيّ شخص في تنفيذ هذا، سواء أكان بقصد أم لا؛ حيث يكفي استخدام برامج بطرق غير قانونية، أو نسخ وتوزيع برامج مُرخّصة دون إذن المالك.

8. يُعدّ تلقي تحذيرات من امتلاء الحاسوب بالفيروسات أحد مؤشرات وجود برامج مقرصنة.

9. يساعد استخدام شبكة افتراضية خاصة (VPN) في إخفاء عنوان IP؛ مما يصعب مهمة وصول مجرمي الإنترنت إلى أجهزة المستخدمين.

10. البرامج المقرصنة هي برامج مُصرَّح بها، يتم نسخها بصورة قانونية بهدف توزيعها أو بيعها دون الحصول على إذن المالك.

11. يؤدي استخدام البرامج المقرصنة إلى عواقب قانونية، مثل الحبس، لكن لا يُشترط دفع غرامات مالية في جميع الحالات.

12. لا يشترط قراءة متطلبات تثبيت البرامج قبل التنزيل؛ طالما تم الأمر عبر متاجر التطبيقات المعتمدة.

التمرين الثالث

اكتب اسم المصطلح المقصود مكان النقاط

1. من غير الصحيح أن ..... يُخفي هوية المستخدِم وسِجِلّ التصفُّح عن مزودي خدمات الإنترنت والحكومات والمعلنين.
2. يساعد برنامج ..... في وضع حدود لتدخلات الآخرين في تحرير محتوى مستند ما.
3. تساعد ..... في التواصل بين زملاء العمل بدلاً من المقابلات المباشرة.
4. ..... هي تطبيقات يمكن استخدامها في جدولة واجبات العمل؛ مما يسهل التعاون بسهولة مع فريق العمل، بغضّ النظر عن المسافة.
5. ..... يُقصَد بها الحصول على برامج غير قانونية أو نشرها عبر الإنترنت.

حلّ التمارين والتدريبات

السـؤال

التمرين الأول: اختر الإجابة الصحيحة

الإجابة

1. جميع ما سبق.
2. حفظ المعلومات الخاصة بالمستخدم على جهاز الحاسوب الخاص به؛ لاستخدامها مجدداً في حال زيارة مواقع الويب.
3. تحميل القرص الصلب.
4. التزوير أو التقليد.
5. التكلفة المالية المنخفضة والتساهل في إجراءات التثبيت.

السـؤال

التمرين الثاني: اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخاطئة، مع تصويب الخطأ:

الإجابة

1. صحيح.
2. صحيح.
3. خطأ؛ رغم تمتع جميع المتصفحات الرئيسية بإعدادات تصفح خاصة، منها: إخفاء سجل التصفح الخاص بالمستخدم عن باقي المستخدمين على نفس جهاز الحاسوب؛ إلا أن الاعتقاد المسيطر على الكثيرين من أن "وضع التصفح المتخفي" incognito mode يخفي هوية المستخدم وسجل التصفح عن مزودي خدمات الإنترنت والحكومات والمعلنين، غير صحيح؛ فهذا الوضع يقوم فقط بمسح السجل الموجود على نظامه، وفائدته تنحصر في إخفاء تفاصيل بحثه في حال استخدام حاسوب عام.
4. صحيح.
5. خطأ؛ تُمكّن المستخدمين من تصنيف البيانات في أعمدة وصفوف وأقسام واضحة تسهل قراءتها وفَهمها.

6. خطأ؛ أدوات إدارة المشاريع.
7. صحيح.
8. صحيح.
9. صحيح.
10. خطأ؛ هي برامج غير مصرَّح بها يتم نسخها بصورة غير قانونية؛ بهدف توزيعها أو بيعها دون الحصول على إذن المالك.
11. خطأ؛ يؤدي استخدام البرامج المقرصنة إلى عواقب قانونية، مثل الغرامات أو حتى السجن في بعض الحالات.
12. خطأ؛ بل يُشترط قراءتها جيداً؛ إذ يمكن أن توجد برامج غير مُرخَّصة أو تتضمَّن فيروسات على المتاجر الرسمية.

السـؤال

التمرين الثالث: اكتب اسم المصطلح المقصود مكان النقاط

الإجابة

1. وضع التصفح المتخفي.
2. معالج النصوص.
3. برامج عقد المؤتمرات عن بُعْد.
4. أدوات إدارة المشاريع.
5. القرصنة عبر الإنترنت.

المراجع

1. Computer program. Follow link: https://www.britannica.com/technology/computer-program
2. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/
3. What is a web browser?. Follow link: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/
4. What are Cookies?. Follow link: https://www.kaspersky.com/resource-center/definitions/cookies
5. What Is Video Conferencing Software?. Follow link: https://www.bigcommerce.com/glossary/video-conferencing-software/
6. Katie Terrell Hanna, spreadsheet. Follow link: https://www.techtarget.com/whatis/definition/spreadsheet
7. Deepak Palasamudram, What is Project Management?, Dec 2022. Follow link: https://2u.pw/RYVwfkV4
8. What is Software Piracy?. Follow link: https://www.javatpoint.com/what-is-software-piracy
9. Software Piracy Facts. Follow link: https://hypertecsp.com/knowledge-base/software-piracy-facts/

10. Investigation: WannaCry cyber attack and the NHS 27 October 2017 https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs

11. What is Pirated Software?. Follow link: https://cyberpedia.reasonlabs.com/EN/pirated%20software.html

12. Devin Partida, Why You Shouldn't Use Pirated Software (But Why People Still Do), 2020. Follow link: https://www.computer.org/publications/tech-news/trends/why-you-shouldnt-use-pirated-software

13. Don't Risk It: The Top 10 Dangers of Downloading Unverified Software, March 2023. Follow link: https://www.lockwell.co/blog/don-t-risk-it-the-top-10-dangers-of-downloading-unverified-software

14. Lital Asher-Dotan, What is the Conficker worm. Follow link: https://www.cybereason.com/blog/what-is-the-conficker-worm

15. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

16. Raja Viswanathan, Remote work, pirated software, and local admin rights: A deadly cocktail. Follow link: https://www.securden.com/blog/pirated-software-malware.html

17. Do You Know How To Spot Fake Software And Updates? Learn The 7 Red Flags!. Follow link: https://www.alvareztg.com/do-you-know-how-to-spot-fake-software-and-updates-learn-the-7-red-flags/

18. Clare Stouffer, Are you accidentally pirating software? ,January 2024. Follow link: https://us.norton.com/blog/malware/accidentally-pirating-software

19. How to check if a file is safe to download. FOLLOW LINK: https://www.microsoft.com/en-us/edge/learning-center/how-to-check-if-a-file-is-safe-to-download?form=MA13I2

20. Microsoft Defender SmartScreen. FOLLOW LINK: https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

21. How Can I Tell If a Download Is Safe?. FOLLOW LINK: https://codesigningstore.com/how-to-tell-a-download-is-safe


الوكالة الوطنية للامن السيبراني
National Cyber Security Agency
الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy
المبادرة الوطنية للسلامة الرقمية
Digital Safety National Initiative