دليل المستخدم لبرنامج الحماية الشامل

كاسبيرسكى بيور 2013

اعداد

شريف .م . عوض

Kaspersky PURE

دليل المستخدم

إصدار التطبيق: 3.0

عزيزي المستخدم،

نشكركم لاختيار منتجنا. ونطمح أن تساعدكم هذه الوثيقة في عملكم وأن تمدكم بإجابات لمعظم تساؤلاتكم التي قد تثار حول هذا البرنامج.

تاريخ مراجعة المستند: 04/12/2012

http://me.kaspersky.com
http://support.kaspersky.com

المحتويات

حول هذا الدليل

هذا المستند هو دليل مستخدم Kaspersky PURE.

لاستخدام Kaspersky PURE بشكل سليم، يجب أن تتعرف على واجهة نظام التشغيل التي تستخدمها، ومعالجة الأساليب الأساسية الخاصة بهذا النظام، ومعرفة كيفية العمل باستخدام البريد الإلكتروني والإنترنت.

فيما يلي يتم توضيح الغرض من هذا الدليل:

- مساعدتك على تثبيت PURE، وتنشيطه، واستخدامه.
- ضمان القيام بعمليات بحث سريعة على للحصول على معلومات حول المشاكل المتعلقة بالتطبيق.
- شرح مصادر المعلومات الأخرى المتعلقة بالتطبيق وطرق تلقي الدعم الفني.

في هذا القسم

في هذا الدليل

تحتوي هذه الوثيقة على الأقسام التالية:

مصادر المعلومات المتعلقة بالتطبيق

يصف هذا القسم مصادر المعلومات الخاصة بالتطبيق وقوائم مواقع الويب التي يمكنك استخدامها لمناقشة تشغيل التطبيق.

Kaspersky PURE

يحتوي هذا القسم على وصف لميزات التطبيق ومعلومات مختصرة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين للتطبيق. ويوفر هذا القسممعلومات حول البرنامج ومتطلبات الأجهزة التي يجب أن تتوفر في الكمبيوتر للسماح للمستخدم بتثبيت التطبيق عليها.

تثبيت التطبيق وإزالته

يحتوي هذا القسم على إرشادات خطوة بخطوة لتثبيت التطبيق وإزالته.

ترخيص التطبيق

يشتمل هذا القسم على معلومات حول المفاهيم الأساسية لتنشيط التطبيق. اقرأ هذا القسم لتتعرف على المزيد حول الهدف من اتفاقية ترخيص المستخدم النهائي، وأنواع التراخيص، وطرق تنشيط التطبيق، وتجديد الترخيص.

تنفيذ المهام المشتركة

يحتوي هذا القسم على إرشادات خطوة بخطوة لتنفيذ المهام التقليدية للمستخدم التي يوفرها التطبيق.

الاتصال بخدمة الدعم الفني

يوفر هذا القسم معلومات حول كيفية الاتصال بالدعم الفني في Kaspersky Lab.

التطبيقات

يوفر هذا القسم معلومات مكملة لنص المستند.

المصطلحات

يحتوي هذا القسم على قائمة بالمصطلحات الواردة في المستند، وتعريفات لكلٍّ منها.

Kaspersky Lab ZAO

يوفر هذا القسم معلومات حول Kaspersky Lab ZAO.

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يوفر هذا القسم معلومات حول الرمز الخاص بالطرف الخارجي والمستخدم في التطبيق.

إشعارات العلامة التجارية

يسرد هذا القسم العلامات التجارية الخاصة بالأطراف الخارجية المصنعة والمستخدمة في هذا المستند.

الفهرس

يتيح لك هذا القسم سرعة العثور على المعلومات المطلوبة داخل هذه الوثيقة.

اصطلاحات الوثيقة

يتضمن نص الوثيقة عناصر دلالية نوصيك بالانتباه لها على وجه الخصوص، وهي: التحذيرات، والتلميحات، والأمثلة.

يتم استخدام اصطلاحات الوثيقة لتمييز العناصر الدلالية. يوضح الجدول التالي اصطلاحات الوثيقة وأمثلة لاستخدامها.

الجدول 1. *اصطلاحات الوثيقة*

نص عينة	وصف اصطلاح الوثيقة
لاحظ...	يتم تمييز التحذيرات باللون الأحمر وتوضع في مربع.
	توفر التحذيرات معلومات حول الإجراءات المتاحة وغير المرغوبة، والتي قد تؤدي إلى فقد البيانات أو حدوث حالات فشل في تشغيل الجهاز أو وجود مشاكل تتعلق بنظام التشغيل.

نص عينة	وصف اصطلاح الوثيقة
نوصيك باستخدام...	يتم وضع الملاحظات في مربع. قد تحتوي الملاحظات على تلميحات مفيدة أو توصيات أو قيم معينة للإعدادات أو حالات خاصة مهمة في تشغيل التطبيق.
مثال: ...	تظهر الأمثلة في صورة مربعات على خلفية صفراء تحمل اسم "مثال".
تحديث يعني... قواعد *البيانات قديمة* وقوع حدث.	يتم كتابة العناصر الدلالية التالية بالخط المائل في النص: • المصطلحات الجديدة • أسماء حالات وأحداث التطبيق
اضغط **إدخال**. اضغط على **ALT+F4**.	تظهر أسماء مفاتيح لوحة المفاتيح بخط عريض وبأحرف كبيرة. أسماء مفاتيح لوحة المفاتيح المتصلة بعلامة "+" (زائد) تشير إلى استخدام توليفة مفاتيح. يجب الضغط على تلك المفاتيح في آن واحد.
انقر فوق زر **تمكين**.	يتم تمييز أسماء عناصر واجهة التطبيق، مثل حقول الإدخال وعناصر القائمة والأزرار بالخط العريض.
لتكوين جدولة المهمة:	تتم كتابة العبارات الافتتاحية للتعليمات بحروف مائلة وتكون مصحوبة بعلامة سهم.
في سطر الأوامر، اكتب help. ستظهر بعد ذلك الرسالة التالية: حدد التاريخ بتنسيق يوم / شهر / سنة .	يتم تمييز الأنواع التالية من المحتوى النصي بكتابتها بخط خاص: • نص في سطر الأوامر • نص الرسائل الذي يعرضه التطبيق على الشاشة • البيانات التي يجب أن يدخلها المستخدم.
<اسم المستخدم>	يتم وضع المتغيرات داخل أقواس زاوية. بدلاً من المتغير، أدخل القيمة المناسبة دون تضمين الأقواس السهمية.

مصادر المعلومات المتعلقة بالتطبيق

يصف هذا القسم مصادر المعلومات الخاصة بالتطبيق وقوائم مواقع الويب التي يمكنك استخدامها لمناقشة تشغيل التطبيق.

يمكنك تحديد أنسب مصدر معلومات، وفقًا لمستوى أهمية وضرورة المشكلة.

في هذا القسم

مصادر معلومات البحث الخاص بك

يمكنك الاتصال بالمصادر التالية للمعلومات للبحث بنفسك:

- صفحة التطبيق على موقع Kaspersky Lab
- صفحة التطبيق على موقع الدعم الفني (قاعدة المعارف)
- تعليمات عبر الإنترنت
- وثائق

إذا لم تتمكن من العثور على حل لمشكلتك بنفسك، فنوصيك بالاتصال بـ الدعم الفني لـ Kaspersky Lab (راجع القسم "فتاها ربع يفنلا معدلا" في صفحة 79).

يجب أن يتوفر لديك اتصالًا بالإنترنت لتتمكن من استخدام المعلومات الموجودة على موقع Kaspersky Lab على الويب.

صفحة التطبيق على موقع **Kaspersky Lab**

يشتمل موقع Kaspersky Lab على صفحة واحدة لكل تطبيق على حدة.

في صفحة الويب (http://www.kaspersky.com/kaspersky-pure) يمكنك عرض معلومات عامة حول التطبيق، والوظائف، والميزات الخاصة به.

تحتوي الصفحة على ارتباط إلى المتجر الإلكتروني. حيث يمكنك شراء التطبيق أو تجديده فيه.

صفحة التطبيق على موقع الدعم الفني (قاعدة المعارف)

قاعدة المعارف هي قسم في موقع الدعم الفني على الويب يوفر نصائح حول استخدام تطبيقات Kaspersky Lab. وتحتوي قاعدة المعارف على مقالات مرجعية مصنفة حسب الموضوع.

على صفحة التطبيق في قاعدة المعارف (http://support.kaspersky.com/pure) يمكنك قراءة مقالات تحوي معلومات وتوصيات وإجابات مفيدة عن الأسئلة الشائعة حول كيفية شراء التطبيق وتثبيته واستخدامه.

قد توفر المقالات إجابات عن أسئلة لا ترتبط ببرنامج Kaspersky PURE، وتكون مرتبطة بتطبيقات Kaspersky Lab أخرى. وقد تحتوي أيضًا على أخبار من خدمة الدعم الفني.

تعليمات عبر الإنترنت

تحتوي التعليمات عبر الإنترنت الخاصة بالتطبيق على ملفات للمساعدة.

تحتوي تعليمات السياق على معلومات حول كل نافذة من نوافذ التطبيق: وهي قوائم تسرد وتصف إعدادات التطبيق والمهام المرتبطة به.

توفر التعليمات الكاملة معلومات حول إدارة حماية الكمبيوتر، وتكوين التطبيق، وحل مشاكل مهام المستخدم النمطية.

وثائق

يوفر دليل المستخدم من Kaspersky PURE معلومات حول طريقة التثبيت والتنشيط والتكوين واستخدام التطبيق. كما تقدم الوثيقة وصفًا لواجهة التطبيق، وتقترح كذلك الطرق لحل مهام المستخدم النمطية أثناء استخدام التطبيق.

مناقشة تطبيقات KASPERSKY LAB في المنتدى

إذا لم يكن سؤالك يتطلب توفير إجابة فورية، يمكنك مناقشته مع خبراء Kaspersky Lab والمستخدمين الآخرين في المنتدى الخاص بنا (http://forum.kaspersky.com).

في هذا المنتدى، يمكنك عرض الموضوعات الموجودة، وترك تعليقاتك، وإنشاء موضوعات جديدة للمناقشة.

الاتصال بإدارة المبيعات

إذا كان لديك أي أسئلة تتعلق بكيفية تحديد أو شراء أو تجديد التطبيق، يمكنك الاتصال بالمتخصصين في قسم المبيعات بأي من الطرق التالية:

- عن طريق الاتصال بمكتبنا الرئيسي في موسكو عبر الهاتف (http://www.kaspersky.com/contacts).
- عن طريق إرسال رسالة تتضمن سؤالك إلى sales@kaspersky.com.

هذه الخدمة متاحة باللغتين الروسية والإنجليزية.

الاتصال بوحدة الكتابة الفنية والترجمة عن طريق البريد الإلكتروني

إذا كانت لديك أي أسئلة حول الوثائق، يرجى التفضل بالاتصال بمجموعة تطوير الوثائق الفنية الخاصة بنا. على سبيل المثال، إذا كنت ترغب في ترك ملاحظات.

يحتوي هذا القسم على وصف لميزات التطبيق ومعلومات مختصرة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين للتطبيق. ويوفر هذا القسممعلومات حول البرنامج ومتطلبات الأجهزة التي يجب أن تتوفر في الكمبيوتر للسماح للمستخدم بتثبيت التطبيق عليها.

في هذا القسم:

ما الجديد

يوفر Kaspersky PURE الميزات الجديدة التالية:

- تمت إضافة الخدمات النقدية الآمنة لضمان الاستخدام الآمن للخدمات البنكية وأنظمة السداد عبر الإنترنت، وكذا تسهيل التسوق عبر الإنترنت (راجع الصفحة 48).
- حماية مُحسَّنة من راصدات لوحة المفاتيح لبيانات الهوية التي تقوم بإدخالها على مواقع الويب:
  - تمت إضافة القسم حماية إدخال البيانات بواسطة لوحة مفاتيح الكمبيوتر (راجع الصفحة 52).
  - يقوم التطبيق تلقائيًا بإضافة زر تشغيل لوحة المفاتيح الظاهرية إلى حقول إدخال كلمات المرور على المواقع (راجع القسم "استخدام لوحة المفاتيح الظاهرية" في الصفحة 50).
- التخزين على الإنترنت متاح الآن لتخزين النُسخ الاحتياطية من الملفات (راجع القسم "استخدام التخزين على الإنترنت" في صفحة 66). يعمل ذلك على تحسين مستوى أمان تخزين البيانات، كما يبسط الوصول إلى البيانات باستخدام التقنية السحابية.
- من أجل توفير الحماية من الدخلاء الذي يستغلون قابلية اختراق البرامج، تمت إضافة ميزة الحماية من الاستغلال إلى مكون مراقب النظام.
- تم تحسين "مدير كلمات المرور". يمكن الآن تخزين قاعدة بيانات كلمات المرور على الخوادم البعيدة. تجعل الآن ميزة المزامنة كلمات المرور وبيانات الهوية الحالية متاحة على كل أجهزة الكمبيوتر المحمولة والمكتبية المُثبَّت عليها Kaspersky PURE.
- تم تحسين واجهة Kaspersky PURE من خلال إضافة تلميحات منبثقة تتضمن نصائح مفيدية لاستخدام التطبيق.
- تم تبسيط إجراء تثبيت التطبيق (راجع القسم "متى يجب إزالة تطبيقات أخرى" في صفحة 17). تمت إضافة خيار التثبيت التلقائي لآخر إصدار من Kaspersky PURE، بما يتضمن مجموعة من آخر التحديثات لقواعد بيانات التطبيق.

- تم تقليل حجم قواعد بيانات التطبيق، الأمر الذي يتيح تقليل حجم البيانات المطلوب تنزيلها وزيادة سرعة تثبيت التحديثات.
- تم تحسين التحليل المساعد على الاكتشاف الذي يتم إجراؤه عند فحص مواقع الويب لاكتشاف الاحتيال.
- تم تعديل رسائل "الرقابة الأسرية" التي تظهر للأطفال بشكل يتلائم معهم. تم تحسين دقة "الرقابة الأسرية": يستخدم الآن هذا المكون التقنية السحابية عند فحص مواقع الويب لاكتشاف المحتوى غير المرغوب فيه.

الوظائف والتطبيقات الرئيسية

يوفر Kaspersky PURE حماية شاملة للكمبيوتر. والحماية الشاملة تعني حماية جهاز الكمبيوتر والبيانات والمستخدم، فضلاً عن إدارة برنامج Kaspersky PURE عن بعد على كل أجهزة الكمبيوتر الموجودة على الشبكة. كما تتوفر وظائف مختلفة ومكونات حماية متنوعة كجزء من Kaspersky PURE من أجل تقديم الحماية الشاملة.

حماية جهاز الكمبيوتر

مكونات الحماية تم تصميمها لحماية الكمبيوتر ضد التهديدات المعروفة والجديدة، وهجمات الشبكات وهجمات الاحتيال، والبريد الإلكتروني غير المرغوب فيه وغيرها من المعلومات غير المرغوب فيها. تتم معالجة كل نوع من التهديدات بواسطة مكون أمان فردي (انظر المزيد عن وصف المكونات في هذا القسم). ويمكن تمكين المكونات أو تعطيلها بصورة مستقلة عن بعضها بالإضافة إلى إمكانية تكوين الإعدادات الخاصة بها.

بالإضافة إلى الحماية الثابتة التي توفرها مكونات الأمان، نوصي بأن تقوم *بفحص* جهاز الكمبيوتر بحثًا عن الفيروسات بصورة منتظمة. وهذا أمر ضروري لإلغاء احتمالية نشر البرامج الخبيثة التي لم تكتشفها مكونات الحماية، على سبيل المثال، بسبب ضبط مستوى الحماية على منخفض أو لأسباب أخرى.

للحفاظ على برنامج Kaspersky PURE محدثًا، يجب عليك *تحديث* قواعد البيانات والوحدات النمطية للبرامج التي يستخدمها التطبيق.

وعند وجود أي شكوك حول أمان أي تطبيق، يمكن تشغيل هذه البنود في *بيئة آمنة*.

يمكن أداء بعض المهام المعينة التي تحتاج لأن يتم أداؤها من وقت لآخر بمساعدة *أدوات ومعالجات إضافية*، مثل تكوين Microsoft® Internet Explorer® وإزالة تتبعات نشاط المستخدم في النظام.

توفر مكونات الحماية التالية حراسة جهاز الكمبيوتر في الوقت الحقيقي:

فيما يلي وصف منطق تشغيل مكونات الحماية في وضع Kaspersky PURE الموصى به من قبل المتخصصين في شركة Kaspersky Lab (مع إعدادات التطبيق الافتراضية).

مكافحة فيروسات الملفات

يقوم مكون مكافحة فيروسات الملفات بمنع إصابة نظام ملفات الكمبيوتر. يبدأ المكون عند بداية نظام التشغيل، وتظل بصورة مستمرة في ذاكرة الوصول العشوائي للكمبيوتر، وتقوم بفحص كل الملفات التي تم فتحها أو تخزينها أو بدؤها على جهاز الكمبيوتر فضلاً عن جميع محركات الأقراص التي تم توصيلها. ويقوم برنامج Kaspersky PURE باعتراض جميع محاولات الوصول إلى أي ملف وفحص الملف بحثًا عن الفيروسات المعروفة. ويمكن إجراء عمليات معالجة أخرى للملف إذا لم يكن مصابًا أو إذا تمت معالجته بنجاح بواسطة التطبيق. إذا تعذر تنظيف ملف ما لأي سبب من الأسباب، فسيتم حذفه. سيتم حفظ نسخة من الملف في النسخ الاحتياطي، أو يتم نقلها إلى العزل.

مكافحة فيروسات البريد

يقوم مكون مكافحة فيروسات البريد بفحص رسائل البريد الإلكتروني الواردة والصادرة على جهاز الكمبيوتر. ويتاح البريد الإلكتروني للمرسل إليه فقط إذا لم يحتو على كائنات خطرة.

مكافحة فيروسات الويب

يعترض مكون مكافحة فيروسات الويب استثناء البرامج النصية الموجودة في مواقع الويب ومنعها إذا ما شكلت تهديدًا. كما يراقب مكون مكافحة فيروسات الويب كل حركة مرور الويب ويمنع الوصول إلى مواقع الويب الخطيرة.

مكافحة فيروسات المراسلة الفورية

يضمن مكون مكافحة فيروسات المراسلة الفورية الاستخدام الآمن لأدوات نداء الإنترنت. ويعمل هذا المكون على حماية المعلومات الواردة إلى جهاز الكمبيوتر عن طريق بروتوكولات المراسلة الفورية. ويضمن مكون مكافحة فيروسات المراسلة الفورية التشغيل الآمن لمختلف تطبيقات المراسلة الفورية.

الدفاع الوقائي

يتيح مكون الدفاع الوقائي إمكانية اكتشاف برنامج خبيث جديد قبل تنفيذ نشاطه الخبيث. ويعتمد تشغيل هذا المكون على مراقبة سلوك كافة التطبيقات المثبتة على جهاز الكمبيوتر وتحليلها. وحسب الإجراءات التي يجري تنفيذها من قِبل التطبيقات، يحدد برنامج Kaspersky PURE ما إذا كان تطبيق ما يحتمل كونه خطرًا أو لا. وبالتالي، لا يكون جهاز الكمبيوتر محميًا ضد الفيروسات المعروفة فقط، بل وأيضًا الفيروسات الجديدة التي لم تكتشف بعد.

التحكم في التطبيق

يسجل مكون التحكم في التطبيق الإجراءات التي تنفذها التطبيقات في النظام، ويدير أنشطة التطبيقات حسب المجموعة التي يعينها المكون لها. ويتم تحديد مجموعة قواعد لكل مجموعة من التطبيقات. حيث يتم بواسطة هذه القواعد إدارة وصول التطبيقات إلى موارد نظام التشغيل المختلفة.

جدار الحماية

يضمن جدار الحماية أمان عملك على الشبكات المحلية وعلى الإنترنت. ويعمل المكون على تصفية كل أنشطة شبكة الاتصال باستخدام نوعين من القواعد: *قواعد التطبيقات* و*قواعد الحزم*.

مراقبة الشبكة

مراقبة الشبكة هي أداة مصممة لمراقبة أنشطة الشبكة في الوقت الحقيقي.

حاجب هجمات الشبكة

يتم تحميل حاجب هجمات شبكة الاتصال عند بدء نظام التشغيل، ويقوم بتتبع حركة شبكة الاتصال الواردة للأنشطة التي تعد مميزة وخاصة بهجمات شبكة الاتصال. عند اكتشاف محاولة هجوم على الكمبيوتر, يقوم برنامج Kaspersky PURE بمنع أي نشاط على الشبكة للكمبيوتر المهاجم ضد الكمبيوتر الخاص بك.

مكافحة البريد الإلكتروني غير المرغوب فيه

يندمج مكون مكافحة البريد الإلكتروني غير المرغوب فيه في عميل البريد المثبت على جهاز الكمبيوتر، ويفحص جميع رسائل البريد الإلكتروني الواردة بحثًا عن البريد الإلكتروني غير المرغوب فيه. ويتم تمييز جميع الرسائل المحتوية على بريد إلكتروني غير مرغوب فيه برأس خاصة. يمكنك تكوين مكون مكافحة البريد الإلكتروني غير المرغوب فيه بحيث يعالج رسائل البريد العشوائي بطريقة خاصة (فيقوم مثلا بحذفها تلقائيًا أو نقلها إلى مجلد خاص).

مكافحة الاحتيال

يقوم مكون مكافحة الاحتيال بفحص عناوين الويب مقابل قوائم تضم مواقع الويب الخبيثة والخادعة. إن هذا المكون هو مكون مندمج مع مكون مكافحة فيروسات الويب، ومكون مكافحة البريد الإلكتروني غير المرغوب فيه، ومكون مكافحة فيروسات المراسلة الفورية.

مكافحة الشعارات

يقوم مكون مكافحة الشعارات بمنع الشعارات الإعلانية التي على مواقع الويب وفي واجهات التطبيق.

الخدمات النقدية الآمنة

توفر الخدمات النقدية الآمنة الحماية للبيانات السرية عند استخدام الخدمات البنكية وأنظمة الدفع على الإنترنت، كما أنها تحول دون سرقة الأصول عند إجراء عمليات الدفع على الإنترنت.

حماية البيانات

تم تصميم ميزات النسخ الاحتياطي وتشفير البيانات ومدير كلمات المرور لحماية البيانات من الفقد أو الوصول غير المصرح به أو السرقة.

نسخة احتياطية

يمكن فقدان البيانات المخزنة على جهاز الكمبيوتر لأسباب مختلفة، مثل التعرض للفيروسات أو تعديل غير مرخص به أو إزالتها من قِبل مستخدم آخر. لتجنب فقدان معلومات مهمة، يجب عليك الاحتفاظ بنسخ احتياطية من البيانات دوريًا.

تنشئ وظيفة النسخ الاحتياطي نسخًا احتياطية للكائنات في تخزين خاص على الجهاز المحدد. وللقيام بذلك، يجب تكوين مهام النسخ الاحتياطي. وبعد تشغيل المهمة يدويًا أو تلقائيًا، وفقًا لجدولة، سوف يتم إنشاء نسخ احتياطية للملفات المحددة في التخزين. وعند الضرورة، يمكن استعادة النسخة المطلوبة من الملف المحفوظ من النسخة الاحتياطية.

تشفير البيانات

تتطلب المعلومات السرية، التي يتم حفظها في وضع إلكتروني، حماية إضافية من الوصول غير المصرح به. ويوفر تخزين البيانات في حاوية مشفرة هذه الحماية.

يتيح تشفير البيانات إنشاء حاويات خاصة مشفرة على القرص الذي تم اختياره. وفي النظام، يتم عرض تلك الحاويات كمحركات أقراص ظاهرية قابلة للإزالة. ويجب أن تقوم بإدخال كلمة مرور ليتم الوصول إلى البيانات المخزنة في حاوية مشفرة.

مدير كلمات المرور

معظم خدمات الإنترنت والموارد تطلب من المستخدمين التسجيل وإدخال تفاصيل تسجيل الدخول. لأسباب أمنية، فمن المستحسن استخدام حسابات مستخدم مختلفة في مواقع مختلفة، واستظهار وتذكر تسجيلات دخول المستخدمين وكلمات المرور من دون كتابتها.

يتيح مدير كلمات المرور تخزين مختلف البيانات الشخصية في صورة مشفرة (على سبيل المثال، أسماء المستخدم وكلمات المرور والعناوين وأرقام الهواتف وأرقام بطاقات الائتمان). ويكون الوصول إلى البيانات محميًا بكلمة مرور رئيسية واحدة. بعد إدخال كلمة المرور الرئيسية، يمكن أن يقوم مدير كلمات المرور بملء حقول نماذج تسجيل الدخول إلى مواقع الويب المختلفة تلقائيًا. تتيح لك كلمة المرور الرئيسية إدارة كل حسابات مواقع الويب الخاصة بك.

الرقابة الأسرية

تم تصميم مكون الرقابة الأسرية لحماية الأطفال والمراهقين من التهديدات المتعلقة باستخدام الكمبيوتر والإنترنت.

يتيح لك مكون الرقابة الأسرية وضع قيود مرنة على وصول مختلف المستخدمين إلى موارد وتطبيقات الإنترنت، كل حسب عمره. كما أنه يمكنك أيضًا من استعراض التقارير الإحصائية حول نشاط المستخدم الذي تتم مراقبته.

التحكم في الشبكة المنزلية

تحتوي شبكة الاتصال المنزلية غالبًا على أجهزة كمبيوتر متعددة، والتي تجعل من الصعب إدارة أمان الشبكة. حيث إن قابلية اختراق أحد الأجهزة يعرض الشبكة كلها للخطر.

يتيح التحكم في الشبكة المنزلية بدء مهام فحص الفيروسات ،وتحديث المهام بجميع الأجهزة أو بأجهزة محددة، كما يقوم بإدارة النسخ الاحتياطي للبيانات، وتكوين إعدادات الرقابة الأسرية على جميع الأجهزة داخل الشبكة من مساحة العمل على الفور. ويضمن هذا إدارة الأمان عن بعد لجميع أجهزة الكمبيوتر داخل شبكة الاتصال المنزلية.

حزمة التوزيع

يمكنك شراء التطبيق بإحدى الطرق التالية:

- **مغلف**. موزع بواسطة المتاجر الخاصة بشركائنا.
- **من متجر الإنترنت**. يتم التوزيع في المتاجر المنتشرة عبر الإنترنت التابعة لـ Kaspersky Lab (مثل، http://me.kaspersky.com أو قسم **المتجر الإلكتروني**)، أو عبر شركات الشركاء.

إذا قمت بشراء الإصدار المغلف من التطبيق، تحتوي حزمة التوزيع على العناصر التالية:

- ظرف محكم الإغلاق يحتوي على القرص المضغوط للإعداد، والذي يحتوي على ملفات التطبيق وملفات الوثائق؛
- دليل مستخدم مختصر يضم رمز التنشيط؛
- اتفاقية ترخيص المستخدم النهائي التي تنص على بنود استخدام التطبيق.

قد يختلف محتوى حزمة التوزيع اعتمادًا على المنطقة التي يتم فيها توزيع التطبيق.

إذا قمت بشراء Kaspersky PURE من متجر عبر الإنترنت، فإنك تقوم بنسخ التطبيق من موقع الويب الخاص بالمتجر. سيتم إرسال معلومات مطلوبة لتنشيط التطبيق إليك عن طريق البريد الإلكتروني بعد أن يتم استلام الدفعة الخاصة بك.

لمزيد من التفاصيل حول طرق الشراء ومجموعة التوزيع، اتصل بإدارة المبيعات من خلال إرسال رسالة إلى sales@kaspersky.com.

خدمة المستخدمين

عن طريق شراء ترخيص للتطبيق، يمكنك الاستفادة من الخدمات التالية طوال فترة صلاحية الترخيص:

- تحديثات قواعد بيانات التطبيق وتحديثات حزمة البرامج
- دعم للمشكلات المرتبطة بالتثبيت والتكوين واستخدام التطبيق بواسطة الهاتف أو بواسطة البريد الإلكتروني
- الإخطارات المتعلقة بإصدار تطبيقات جديدة من Kaspersky Lab، وكذلك المتعلقة بالفيروسات الجديدة وانتشار الفيروسات. لاستخدام هذه الخدمة، اشترك في استلام الأخبار من Kaspersky Lab على موقع ويب الدعم الفني.

لن يتم تقديم نصائح حول المشكلات المرتبطة بأنظمة التشغيل وتطبيقات الأطراف الخارجية والتقنيات.

متطلبات الأجهزة والبرامج

لضمان عمل Kaspersky PURE، ينبغي أن يفي الكمبيوتر بالمتطلبات التالية:

متطلبات عامة:

- 700 ميجابايت كمساحة خالية على محرك الأقراص الصلبة.
- محرك أقراص CD / DVD-ROM (لتثبيت Kaspersky PURE من القرص المضغوط الخاص بالتثبيت).
- ماوس كمبيوتر.
- اتصال بالإنترنت (لتنشيط التطبيق وتحديث قواعد البيانات والوحدات النمطية للتطبيق).
- متصفح Microsoft Internet Explorer 8.0 أو إصدار أحدث
- Microsoft Windows® Installer 3.0.

المتطلبات الخاصة بإصدارات أنظمة التشغيل Microsoft Windows XP Home Edition (Service Pack 3 أو أعلى)، Microsoft Windows XP Professional (Service Pack 3 أو أعلى)، Microsoft Windows XP Professional x64 Edition (Service Pack 2 أو أعلى):

- معالج Intel® Pentium® 800 ميجا هرتز 32 بت (x86 / 64 بت) (x64) أو أعلى (أو مكافئ متوافق).
- ذاكرة وصول عشوائي خالية قدرها 512 ميجا بايت

متطلبات أنظمة التشغيل Microsoft Windows Vista® Home Basic (Service Pack 2 أو أعلى)، Microsoft Windows Vista Home Premium (Service Pack 2 أو أعلى)، Microsoft Windows Vista Business (Service Pack 2 أو أعلى)، Microsoft Windows Vista Enterprise (Service Pack 2 أو أعلى)، Microsoft Windows Vista Ultimate (Service Pack 2 أو أعلى)، Microsoft Windows 7 Starter (Service Pack 1 أو أعلى)، Microsoft Windows 7 Home Basic (Service Pack 1 أو أعلى)، Microsoft Windows 7 Home Premium (Service Pack 1 أو أعلى)، Microsoft Windows 7 Professional (Service Pack 1 أو أعلى)، Microsoft Windows 7 Ultimate (Service Pack 1 أو أعلى)، Windows 8، Microsoft Windows 8 Pro، Microsoft Windows 8 Enterprise أو أعلى (x32 وx64):

- معالج Intel Pentium 1 جيجا هرتز 32 بت (x86 / 64 بت) (x64) أو ما يليه (أو مكافئ متوافق).
- 1 جيجابايت من المساحة الخالية بذاكرة الوصول العشوائي (RAM) (نظام التشغيل 32 بت)؛ 2 جيجابايت من المساحة الخالية بذاكرة الوصول العشوائي (RAM) (نظام التشغيل 64 بت).

متطلبات الحواسب المحمولة:

- معالج Intel Atom™ بقدرة 1.6 جيجاهرتز (Z520) أو معالج مكافئ متوافق.
- 1 جيجا بايت من ذاكرة الوصول العشوائي.
- محول فيديو Intel GMA950 بذاكرة لا تقل عن 64 ميجابايت (أو محول مكافئ متوافق).
- شاشة مقاس 10.1 بوصات كحد أدنى.

لا يدعم التطبيق "مدير كلمات المرور" في أنظمة التشغيل 64 بت.

تثبيت التطبيق وإزالته

يحتوي هذا القسم على إرشادات خطوة بخطوة لتثبيت التطبيق وإزالته.

في هذا القسم:

تثبيت التطبيق

سيتم تثبيت برنامج Kaspersky PURE على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

إذا كان الهدف من التطبيق هو حماية أكثر من كمبيوتر واحد (وفقًا للحد الأقصى لعدد أجهزة الكمبيوتر الذي تحدده بنود اتفاقية ترخيص المستخدم النهائي)، يجب التثبيت بشكل متطابق على جميع أجهزة الكمبيوتر.

لتثبيت برنامج Kaspersky PURE على جهاز الكمبيوتر،

قم بتشغيل ملف الإعداد (ملف بامتداد *.exe) من على القرص المدمج الذي يحتوي على المنتج.

لتثبيت Kaspersky PURE، يمكنك أيضًا استخدام حزمة توزيع يتم تنزيلها من الإنترنت. يعرض معالج الإعداد عدة خطوات إضافية للتثبيت لبعض اللغات المترجمة.

في هذا القسم:

الخطوة 1. العثور على إصدار أحدث من التطبيق

قبل الإعداد، يفحص معالج الإعداد خوادم التحديث في Kaspersky Lab بحثًا عن إصدار أحدث من برنامج Kaspersky PURE.

وفي حالة عدم وجود إصدارات أحدث من البرنامج على خوادم التحديث الخاصة بـ Kaspersky Lab، سيتم بدء تشغيل معالج الإعداد الخاص بالنسخة الحالية.

إذا عرضت خوادم التحديث إصدارًا أحدث من برنامج Kaspersky PURE، سيظهر لك طلب لتحميل هذا الإصدار وتثبيته على الكمبيوتر. يوصى بتثبيت الإصدار الحديث من التطبيق، لأن الإصدارات الأحدث تتضمن المزيد من التحسينات التي تسمح لك بضمان الحصول على حماية أفضل للكمبيوتر الخاص بك. في حالة قيامك بإلغاء تنزيل الإصدار الأحدث، سيتم بدء تشغيل معالج الإعداد الخاص بالإصدار الحالي. أما إذا قررت تثبيت الإصدار الأحدث من التطبيق، فسوف يتم تحميل ملفات توزيع المنتج إلى

جهاز الكمبيوتر وسيبدأ تشغيل معالج الإعداد تلقائياً لتثبيت الإصدار الأحدث. وللمزيد من الوصف الخاص بإجراء التثبيت للإصدار الأحدث، الرجاء الرجوع إلى الوثائق المتوافقة.

الخطوة 2. بدء تثبيت التطبيق

في هذه الخطوة، يعرض عليك معالج الإعداد تثبيت التطبيق.

لمتابعة التثبيت، انقر زر **تثبيت**.

حسب نوع التثبيت ولغة الترجمة، يعرض عليك المعالج في هذه الخطوة إمكانية إظهار اتفاقية الترخيص بينك وبين Kaspersky Lab، كما أنه يعرض عليك إمكانية المشاركة في شبكة أمان Kaspersky.

الخطوة 3. مراجعة اتفاقية ترخيص المستخدم النهائي

في هذه الخطوة، ينبغي عليك مراجعة اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab.

اقرأ اتفاقية ترخيص المستخدم النهائي كاملة، وإذا كنت توافق على جميع الشروط الخاصة بها، فانقر فوق زر **قبول**. سوف يستمر تثبيت التطبيق.

في حالة عدم قبول اتفاقية ترخيص المستخدم النهائي، لن يتم تثبيت التطبيق.

الخطوة 4. بيان تجميع بيانات شبكة أمان KASPERSKY

عند هذه الخطوة، سيدعوك معالج الإعداد للمشاركة في شبكة أمان Kaspersky. تتضمن المشاركة في البرنامج إرسال معلومات حول التهديدات الجديدة المكتشفة على الكمبيوتر الخاص بك والتطبيقات الموجودة قيد التشغيل والتطبيقات الموقعة المنزلة إلى Kaspersky Lab، بجانب المعلومات الخاصة بالنظام الخاص بك. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

استعراض بيان جمع بيانات شبكة اتصال أمان Kaspersky. إذا كنت توافق على جميع بنود الاتفاقية، فحدد خانة الاختيار **أرغب في الاشتراك في شبكة اتصال أمان Kaspersky لتوفير الحماية المثلى لجهاز الكمبيوتر الخاص بي** في نافذة المعالج.

انقر فوق زر **التالي** لمتابعة تثبيت المعالج.

الخطوة 5. التثبيت

قد يستغرق تثبيت التطبيق بعض الوقت. الرجاء الانتظار حتى يكتمل.

وبمجرد أن ينتهي التثبيت، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

يقوم Kaspersky PURE بتنفيذ عمليات فحص متعددة أثناء التثبيت. قد ينتج عن عمليات الفحص هذه اكتشاف المشاكل التالية:

- **عدم توافق نظام التشغيل مع متطلبات البرنامج**. أثناء التثبيت، يقوم المعالج بفحص الحالات التالية:
  - استيفاء نظام التشغيل وحزم الخدمات لمتطلبات تثبيت البرنامج
  - توفر جميع التطبيقات المطلوبة
  - ما إذا كانت المساحة الحرة المتوفرة على القرص كافية للتثبيت

في حالة عدم استيفاء أي من المتطلبات المدرجة أعلاه، سيظهر على الشاشة إخطار يفيد بذلك.

- **توجد تطبيقات غير متوافقة على الكمبيوتر**. في حالة اكتشاف هذه التطبيقات، تظهر القائمة الخاصة بها ويتم عرض إزالتها على المستخدم. تطبيقات لا يستطيع Kaspersky PURE إزالتها بشكل تلقائي، وينبغي إزالتها يدويًا. أثناء إزالة التطبيقات غير المتوافقة، سيتوجب عليك إعادة تشغيل نظام التشغيل، وبعد ذلك ستستمر عملية تثبيت برنامج Kaspersky PURE تلقائيًا.

- **توجد برامج ضارة على الكمبيوتر**. في حالة اكتشاف وجود أي تطبيقات خبيثة تتعارض مع البرامج المكافحة للفيروسات على الكمبيوتر، يطالبك معالج الإعداد بتنزيل الأداة المكتشفة المصممة لإبطال الإصابة وتسمى بأداة *Kaspersky* لإزالة الفيروسات.

إذا وافقت على تثبيت الأداة المساعدة، فإن معالج التثبيت سيقوم بتحميلها من خوادم Kaspersky Lab وبعد ذلك يبدأ في تثبيت الأداة تلقائيًا. إذا لم يتمكن المعالج من تحميل الأداة، سيطلب منك تحميلها بنفسك عن طريق النقر على الارتباط الذي تم توفيره.

الخطوة 6. إكمال التثبيت

في هذه الخطوة، يخبرك المعالج باكتمال تثبيت التطبيق. لتشغيل Kaspersky PURE في الحال، تأكد من تحديد خانة الاختيار **تشغيل Kaspersky PURE 3.0**، وانقر فوق زر **إنهاء**.

في بعض الحالات، قد تحتاج إلى إعادة تشغيل نظام التشغيل لإكمال التثبيت. في حالة تحديد خانة الاختيار **تشغيل Kaspersky PURE 3.0**، يتم بدء تشغيل التطبيق تلقائيًا بعد إعادة تشغيل نظام التشغيل.

في حالة عدم تحديد خانة الاختيار **تشغيل Kaspersky Internet Security 3.0** قبل إغلاق المعالج، ستحتاج إلى بدء تشغيل التطبيق يدويًا.

الخطوة 7. تنشيط التطبيق

عند هذه الخطوة، يعرض عليك معالج الإعداد تنشيط التطبيق.

يعتبر التنشيط عبارة عن عملية يتم من خلالها تنشيط الإصدار كامل لوظائف من التطبيق لفترة محددة من الوقت.

ستحتاج إلى الاتصال بالإنترنت لتنشيط التطبيق.

سُتعرض عليك الخيارات التالية لتنشيط برنامج Kaspersky PURE:

- **تفعيل الإصدار التجاري**. قم بتحديد هذا الخيار وإدخال رمز التنشيط (راجع القسم "طيشنتلا زمر لوح" في صفحة 28) في حالة شراء إصدار تجاري من التطبيق.

- **تفعيل الإصدار التجريبي**. استخدم خيار التنشيط هذا إذا أردت تثبيت الإصدار التجريبي من التطبيق قبل اتخاذ قرار بشراء إصدار تجاري. سيكون بإمكانك استخدام الإصدار كامل الوظائف من التطبيق خلال المدة الزمنية المحددة بموجب الترخيص التجريبي. عند انتهاء مدة الترخيص، يتعذر تنشيطه لمرة ثانية.

الخطوة 8. تسجيل المستخدم

تكون هذه الخطوة متاحة فقط عند تنشيط الإصدار التجاري من التطبيق. عند تنشيط الإصدار التجريبي، يتم تخطي هذه الخطوة.

يستطيع المستخدمون المسجلون إرسال طلبات إلى خدمة الدعم الفني ومعمل مكافحة الفيروسات من خلال حسابي في Kaspersky الموجود على موقع Kaspersky Lab على الويب، بالإضافة إلى إدارة رموز التنشيط بسهولة واستلام أحدث المعلومات الخاصة بالمنتجات الجديدة والعروض الخاصة.

إذا وافقت على التسجيل، قم بتحديد بيانات التسجيل في الحقول المقابلة ثم النقر فوق الزر **التالي** لإرسال البيانات إلى Kaspersky Lab.

الخطوة 9. استكمال التنشيط

يقوم المعالج بإخطارك بنجاح تنشيط Kaspersky PURE. كذلك، يتم توفير معلومات حول الترخيص النشط في هذه النافذة: نوع الترخيص (تجاري أم تجريبي)، تاريخ انتهاء الصلاحية، عدد المضيفات المغطاه بواسطة الترخيص.

إذا كنت تستخدم اشتراكًا، فسيتم عرض المعلومات عن حالة الاشتراك بدلاً من تاريخ انتهاء الترخيص.

انقر الزر **إنهاء** لإغلاق المعالج.

ترقية الإصدار السابق من KASPERSKY PURE

إذا كان لديك الإصدار السابق من PURE مُثبَّتًا على الكمبيوتر، فإنك تحتاج إلى ترقية التطبيق إلى الإصدار الجديد من PURE. إذا كان لديك ترخيص حالي لبرنامج Kaspersky PURE، فلن تضطر إلى التطبيق: سيقوم معالج الإعداد تلقائيًا باسترداد المعلومات الخاصة بترخيص Kaspersky PURE وتطبيقها خلال عملية التثبيت.

سيتم تثبيت برنامج Kaspersky PURE على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

إذا كان الهدف من التطبيق هو حماية أكثر من كمبيوتر واحد (وفقًا للحد الأقصى لعدد أجهزة الكمبيوتر الذي تحدده بنود اتفاقية ترخيص المستخدم النهائي)، يجب التثبيت بشكل متطابق على جميع أجهزة الكمبيوتر.

لتثبيت برنامج Kaspersky PURE على جهاز الكمبيوتر،

قم بتشغيل ملف الإعداد (ملف بامتداد *.exe) من على القرص المدمج الذي يحتوي على المنتج.

لتثبيت Kaspersky PURE، يمكنك أيضًا استخدام حزمة توزيع يتم تنزيلها من الإنترنت. يعرض معالج الإعداد عدة خطوات إضافية للتثبيت لبعض اللغات المترجمة.

في هذا القسم:

الخطوة 1. العثور على إصدار أحدث من التطبيق

قبل الإعداد، يفحص معالج الإعداد خوادم التحديث في Kaspersky Lab بحثًا عن إصدار أحدث من برنامج Kaspersky PURE.

وفي حالة عدم وجود إصدارات أحدث من البرنامج على خوادم التحديث الخاصة بـ Kaspersky Lab، سيتم بدء تشغيل معالج الإعداد الخاص بالنسخة الحالية.

إذا عرضت خوادم التحديث إصدارًا أحدث من برنامج Kaspersky PURE، سيظهر لك طلب لتحميل هذا الإصدار وتثبيته على الكمبيوتر. يوصى بتثبيت الإصدار الحديث من التطبيق، لأن الإصدارات الأحدث تتضمن المزيد من التحسينات التي تسمح لك بضمان الحصول على حماية أفضل للكمبيوتر الخاص بك. في حالة قيامك بإلغاء تنزيل الإصدار الأحدث، سيتم بدء تشغيل معالج الإعداد الخاص بالإصدار الحالي. أما إذا قررت تثبيت الإصدار الأحدث من التطبيق، فسوف يتم تحميل ملفات توزيع المنتج إلى جهاز الكمبيوتر وسيبدأ تشغيل معالج الإعداد تلقائياً لتثبيت الإصدار الأحدث. وللمزيد من الوصف الخاص بإجراء التثبيت للإصدار الأحدث، الرجاء الرجوع إلى الوثائق المتوافقة.

الخطوة 2. بدء تثبيت التطبيق

في هذه الخطوة، يعرض عليك معالج الإعداد تثبيت التطبيق.

لمتابعة التثبيت، انقر زر **تثبيت**.

حسب نوع التثبيت ولغة الترجمة، يعرض عليك المعالج في هذه الخطوة إمكانية إظهار اتفاقية الترخيص بينك وبين Kaspersky Lab، كما أنه يعرض عليك إمكانية المشاركة في شبكة أمان Kaspersky.

الخطوة 3. مراجعة اتفاقية ترخيص المستخدم النهائي

في هذه الخطوة، ينبغي عليك مراجعة اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab.

اقرأ اتفاقية ترخيص المستخدم النهائي كاملة، وإذا كنت توافق على جميع الشروط الخاصة بها، فانقر فوق زر **قبول**. سوف يستمر تثبيت التطبيق.

في حالة عدم قبول اتفاقية ترخيص المستخدم النهائي، لن يتم تثبيت التطبيق.

الخطوة 4. بيان تجميع بيانات شبكة أمان KASPERSKY

عند هذه الخطوة، سيدعوك معالج الإعداد للمشاركة في شبكة أمان Kaspersky. تتضمن المشاركة في البرنامج إرسال معلومات حول التهديدات الجديدة المكتشفة على الكمبيوتر الخاص بك والتطبيقات الموجودة قيد التشغيل والتطبيقات الموقعة المنزلة إلى Kaspersky Lab، بجانب المعلومات الخاصة بالنظام الخاص بك. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

استعراض بيان جمع بيانات شبكة اتصال أمان Kaspersky. إذا كنت توافق على جميع بنود الاتفاقية، فحدد خانة الاختيار **أرغب في الاشتراك في شبكة اتصال أمان Kaspersky لتوفير الحماية المثلى لجهاز الكمبيوتر الخاص بي** في نافذة المعالج.

انقر فوق زر **التالي** لمتابعة تثبيت المعالج.

الخطوة 5. التثبيت

قد يستغرق تثبيت التطبيق بعض الوقت. الرجاء الانتظار حتى يكتمل.

وبمجرد أن ينتهي التثبيت، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

يقوم Kaspersky PURE بتنفيذ عمليات فحص متعددة أثناء التثبيت. قد ينتج عن عمليات الفحص هذه اكتشاف المشاكل التالية:

- **عدم توافق نظام التشغيل مع متطلبات البرنامج**. أثناء التثبيت، يقوم المعالج بفحص الحالات التالية:
  - استيفاء نظام التشغيل وحزم الخدمات لمتطلبات تثبيت البرنامج
  - توفر جميع التطبيقات المطلوبة
  - ما إذا كانت المساحة الحرة المتوفرة على القرص كافية للتثبيت

  في حالة عدم استيفاء أي من المتطلبات المدرجة أعلاه، سيظهر على الشاشة إخطار يفيد بذلك.
- **توجد تطبيقات غير متوافقة على الكمبيوتر**. في حالة اكتشاف هذه التطبيقات، تظهر القائمة الخاصة بها ويتم عرض إزالتها على المستخدم. تطبيقات لا يستطيع Kaspersky PURE إزالتها بشكل تلقائي، وينبغي إزالتها يدويًا. أثناء إزالة التطبيقات غير المتوافقة، سيتوجب عليك إعادة تشغيل نظام التشغيل، وبعد ذلك ستستمر عملية تثبيت برنامج Kaspersky PURE تلقائيًا.
- **توجد برامج ضارة على الكمبيوتر**. في حالة اكتشاف وجود أي تطبيقات خبيثة تتعارض مع البرامج المكافحة للفيروسات على الكمبيوتر، يطالبك معالج الإعداد بتنزيل الأداة المكتشفة المصممة لإبطال الإصابة وتسمى بأداة *Kaspersky* لإزالة الفيروسات.

إذا وافقت على تثبيت الأداة المساعدة، فإن معالج التثبيت سيقوم بتحميلها من خوادم Kaspersky Lab وبعد ذلك يبدأ في تثبيت الأداة تلقائيًا. إذا لم يتمكن المعالج من تحميل الأداة، سيطلب منك تحميلها بنفسك عن طريق النقر على الارتباط الذي تم توفيره.

الخطوة 6. إكمال التثبيت

تخبرك نافذة المعالج هذه باكتمال تثبيت التطبيق بنجاح.

أعد تشغيل نظام التشغيل بعد أن يتم تثبيت التطبيق.

عند تحديد خانة الاختيار **تشغيل Kaspersky PURE 3.0**، سيتم تشغيل التطبيق تلقائيًا بعد إعادة تشغيل نظام التشغيل.

في حالة عدم تحديد خانة الاختيار **تشغيل Kaspersky PURE 3.0** قبل إغلاق المعالج، ستحتاج إلى تشغيل التطبيق يدويًا.

إزالة التطبيق

بعد إزالة تثبيت Kaspersky PURE، سيصبح الكمبيوتر والبيانات الشخصية غير محمية.

تتم إزالة تثبيت Kaspersky PURE من خلال معالج الإعداد.

لتشغيل المعالج،

من قائمة **ابدأ**، حدد **البرامج** → **Kaspersky PURE 3.0** → **إزالة Kaspersky PURE 3.0**.

في هذا القسم:

الخطوة 1. حفظ البيانات للاستخدام في المستقبل

في هذه المرحلة، يمكنك تحديد بيانات التطبيق التي يجب حفظها للاستخدام في المستقبل أثناء عمليات التثبيت اللاحقة للتطبيق (على سبيل المثال، الإصدار الأحدث).

يمكنك تحديد أنواع البيانات التالية للاستخدام مستقبلاً:

- **معلومات الترخيص** – مجموعة من البيانات التي تحدد الحاجة إلى تنشيط التطبيق الجديد عن طريق السماح لك باستخدام الترخيص النشط ما لم تنتهي صلاحية الترخيص قبل بدء التثبيت.
- **كائنات العزل** – الملفات التي يتم فحصها بواسطة التطبيقات ووضعها في "النسخ الاحتياطي" أو "العزل".

بعد أن تتم إزالة Kaspersky PURE من الكمبيوتر، تصبح الملفات المعزولة غير متوفرة. ينبغي تثبيت Kaspersky PURE لتتمكن من معالجة هذه الملفات.

- **إعدادات تشغيل التطبيق** – قيم إعدادات التطبيق المحددة أثناء التكوين.

لا تدعم Kaspersky Lab إعدادات الإصدارات السابقة من التطبيق. بعد تثبيت الإصدار الجديد، نوصي بالتحقق من صحة إعداداته.

- **بيانات iChecker** هي ملفات تتضمن معلومات حول الكائنات التي تم فحصها بالفعل من خلال تقنية iChecker.
- **الحاويات المشفرة (بما في ذلك البيانات)** – ملفات تم نقلها إلى حاويات مشفرة باستخدام ميزة "تشفير البيانات".
- **قواعد بيانات إدارة كلمات المرور (لجميع المستخدمين)** – حسابات المستخدمين والملاحظات الشخصية والإشارات المرجعية وبطاقات الأعمال التي تم إنشاؤها باستخدام ميزة إدارة كلمات المرور.
- **قواعد بيانات مكافحة البريد الإلكتروني غير المرغوب فيه** – هي قواعد بيانات تحتوي على أمثلة لرسائل البريد الإلكتروني غير المرغوب فيها ويتم حفظها بواسطة التطبيق.

بشكل افتراضي، يطالبك التطبيق بحفظ المعلومات الخاصة بالتنشيط.

لحفظ البيانات لاستخدامها مستقبلاً

حدد خانات الاختيار الخاصة بأنواع البيانات التي تريد حفظها.

الخطوة 2. تأكيد الإزالة

لأن إزالة التطبيق يهدد أمان جهاز الكمبيوتر والبيانات الشخصية، سيطلب من المستخدم التأكيد على رغبته في إزالة التطبيق. انقر فوق زر **حذف** لتنفيذ هذا الأمر.

الخطوة 3. إزالة التطبيق. استكمال الإزالة

عند هذه المرحلة، يقوم معالج الإعداد بإزالة التطبيق من على الكمبيوتر. انتظر حتى انتهاء عملية الإزالة.

عند إزالة التطبيق، سيتعين عليك إعادة تمهيد نظام التشغيل الخاص بك. إذا قمت بإلغاء إعادة التمهيد الفورية، فسيتم تأجيل اكتمال إجراء إزالة التطبيق حتى يتم إعادة تمهيد نظام التشغيل، أو يتم إيقاف تشغيل جهاز الكمبيوتر ثم يعاد تشغيله.

ترخيص التطبيق

يشتمل هذا القسم على معلومات حول المفاهيم الأساسية لتنشيط التطبيق. اقرأ هذا القسم لتتعرف على المزيد حول الهدف من اتفاقية ترخيص المستخدم النهائي، وأنواع التراخيص، وطرق تنشيط التطبيق، وتجديد الترخيص.

في هذا القسم:

حول اتفاقية ترخيص المستخدم النهائي

اتفاقية ترخيص المستخدم النهائي هي اتفاقية إلزامية بينك وبين Kaspersky Lab ZAO تحدد البنود التي يمكنك بموجبها استخدام التطبيق.

اقرأ بنود اتفاقية ترخيص المستخدم النهائي بعناية قبل أن تقوم ببدء استخدام التطبيق.

تُعتبر موافقًا على بنود اتفاقية الترخيص بعد تأكيد موافقتك على اتفاقية الترخيص عند تثبيت التطبيق. إذا لم توافق على بنود اتفاقية الترخيص، فيجب أن تقوم بإنهاء عملية تثبيت التطبيق أو أن تمتنع عن استخدام التطبيق.

حول الترخيص

الترخيص هو حق استخدام التطبيق لفترة زمنية محدودة، والذي يتم منحه بموجب اتفاقية ترخيص المستخدم النهائي. ويحدد الترخيص رمز تنشيط فريدًا لنسختك من Kaspersky PURE.

يمنحك الترخيص الحالي الحق في التمتع بأنواع الخدمات التالية:

- الحق في استخدام التطبيق على جهاز واحد أو عدة أجهزة.

يتم تحديد عدد الأجهزة التي قد تستخدم التطبيق عليها في اتفاقية ترخيص المستخدم النهائي.

- المساعدة من قسم الدعم الفني بشركة Kaspersky Lab.
- تتوفر خدمات أخرى من Kaspersky Lab أو شركائها أثناء فترة الترخيص (راجع القسم "خدمات المستخدمين" على الصفحة 15).

يعتمد نطاق فترة استخدام الخدمات والتطبيق على نوع الترخيص المستخدم لتنشيط التطبيق.

يتم توفير أنواع الترخيص التالية:

- *تجريبي* – ترخيص مجاني بهدف تجربة التطبيق.

عادة تكون صلاحية الترخيص المجاني عبارة عن فترة قصيرة. وبمجرد انتهاء صلاحية الترخيص، يتم تعطيل جميع ميزات Kaspersky PURE. لمتابعة استخدام التطبيق، يجب أن تقوم بشراء ترخيص تجاري.

- *تجاري* – ترخيص مدفوع يتم تقديمه عند شراء التطبيق..

عند انتهاء صلاحية الترخيص التجاري، يستمر التطبيق في العمل، ولكن بوظائف محدودة (فلا يمكن إجراء التحديث واستخدام شبكة أمان Kaspersky مثلاً). ولا يزال بإمكانك الاستفادة من كل مكونات التطبيق وتنفيذ عمليات الفحص بحثًا عن الفيروسات والبرمجيات الخبيثة الأخرى، ولكن يتم ذلك فقط باستخدام آخر قواعد بيانات تم تثبيتها قبل انتهاء صلاحية الترخيص. لمتابعة استخدام Kaspersky PURE في وضع الوظائف الكاملة، يجب أن تقوم بتجديد الترخيص التجاري.

نحن نوصيك بتجديد الترخيص قبل انتهاء فترة الصلاحية لضمان الحصول على الحد الأقصى لحماية الكمبيوتر الخاص بك ضد جميع التهديدات الأمنية.

حول توفير البيانات

لزيادة مستوى الحماية، ومن خلال موافقتك على شروط اتفاقية الترخيص، فإنك توافق على توفير المعلومات التالية لـ Kaspersky Lab في الوضع التلقائي:

- معلومات حول المجاميع الاختبارية للملفات التي تتم معالجتها (MD5)؛
- المعلوماتاللازمة لتقييم سمعة عناوين URL؛
- إحصائيات استخدام إخطارات المنتج؛
- البيانات الاحصائية للحماية من البريد الإلكتروني غير المرغوب فيه؛
- بيانات حول تنشيط Kaspersky PURE والإصدار المستخدم حاليًا؛
- معلومات حول أنواع التهديدات المكتشفة؛
- معلومات حول الشهادات الرقمية المستخدمة حاليًا والمعلومات اللازمة للتحقق منها.

إذا كان الكمبيوتر مزوَّدًا بالوحدة النمطية للنظام الأساسي الموثوق به (TPM)، فإنك توافق أيضًا على تزويد Kaspersky Lab بتقرير TPM حول عملية بدء تشغيل نظام التشغيل والمعلومات اللازمة للتحقق منها. إذا حدث خطأ أثناء تثبيت Kaspersky PURE، فإنك توافق على تزويد Kaspersky Lab تلقائيًا لمعلومات حول رمز الخطأ، وحزمة التثبيت المستخدمة حاليًا، والكمبيوتر.

عند المشاركة في شبكة أمان Kaspersky ، يتم بشكل تلقائي إرسال المعلومات التالية - التي يتم إنشاؤها أثناء عمل Kaspersky PURE - إلى Kaspersky Lab:

- معلومات حول المكونات المادية للكمبيوتر والبرامج المُثبَّتة عليه؛
- معلومات حول حالية الحماية من الفيروسات التي عليها الكمبيوتر، إلى جانب الكائنات والإجراءات المحتمل كونها خبيثة، والقرارات المتخذة بخصوص هذه الكائنات والإجراءات؛
- معلومات حول التطبيقات الجاري تنزيلها وتشغيلها؛
- معلومات حول أخطاء الواجهة واستخدام واجهة Kaspersky PURE؛
- معلومات حول إصدار قواعد البيانات المستخدمة حاليًا؛
- إحصائيات التحديثات والاتصالات بخوادم Kaspersky Lab؛

- إحصائيات الوقت الفعلي الذي تستغرقه مكونات التطبيق في فحص الكائنات.

علاوةً على ذلك، قد يتطلب الفحص الإضافي في Kaspersky Lab إرسال الملفات (أو أجزاء منها) المعرضة لخطر استغلال كبير من قِبل الدخلاء للإضرار بكمبيوتر المستخدم أو بياناته.

يحمي Kaspersky Lab أي معلومات يستلمها بهذه الطريقة بموجب نصوص القانون.. تستخدم Kaspersky Lab أي معلومات يتم استردادها كإحصائيات عامة فقط. يتم بشكل تلقائي إنشاء الإحصائيات العامة باستخدام المعلومات الأصلية المستردَّدة، ولا تتضمن أي معلومات خاصة أو معلومات سرية أخرى. يتم تخزين المعلومات الأصلية المستردَّدة بصيغة مشفرة؛ ويتم مسحها كما تم جمعها (مرتان كل عام). يتم تخزين الإحصائيات العامة بشكل غير محدود.

حول رمز التنشيط

يعتبر *رمز التنشيط* عبارة عن رمز تستلمه عند شراء الترخيص التجاري لـ Kaspersky PURE. وهو مطلوب لتنشيط التطبيق.

يعتبر رمز التنشيط عبارة عن سلسلة فريدة مكونة من عشرين رقم وأحرف لاتينية في تنسيق xxxxx-xxxxx-xxxxx-xxxxx.

واعتمادًا على طريقة شراء التطبيق، يمكنك الحصول على رمز التنشيط بأي من الطرق التالية:

- عند شراء الإصدار المعلب من برنامج Kaspersky PURE، يتم توفير رمز التنشيط في الدليل أو على العلبة التي تحتوي على القرص المضغوط الخاص بالتثبيت.
- عند شراء Kaspersky PURE من متجر على الإنترنت، يتم إرسال رمز التنشيط عبر البريد الإلكتروني إلى العنوان الذي تحدده عند طلب الشراء.

يبدأ العد التنازلي لفترة الترخيص من تاريخ تنشيط التطبيق. إذا قمت بشراء ترخيص مخصص لاستخدام Kaspersky PURE على أجهزة متعددة، يبدأ العد التنازلي لفترة صلاحية الترخيص من لحظة تطبيق رمز التنشيط.

في حالة فقدان رمز التنشيط أو حذفه دون قصد، بعد القيام بالتنشيط، اتصل بخدمة دعم Kaspersky Lab الفني لاستعادته.

تنفيذ المهام المشتركة

يحتوي هذا القسم على إرشادات خطوة بخطوة لتنفيذ المهام التقليدية للمستخدم التي يوفرها التطبيق.

في هذا القسم:

تنشيط التطبيق

تحتاج إلى تنشيط التطبيق لتتمكن من استخدام وظائفه والخدمات المقترنة بها.

إذا لم تقم بتنشيط التطبيق أثناء التثبيت، يمكنك تنفيذ هذا الأمر لاحقًا. سيتم تذكيرك بالحاجة إلى تنشيط التطبيق بواسطة رسائل Kaspersky PURE التي تظهر في منطقة إخطارات شريط المهام. يتم تنشيط Kaspersky PURE باستخدام معالج التنشيط.

لتشغيل معالج تنشيط برنامج Kaspersky PURE، قم بتنفيذ أحد الإجراءات التالية:

- انقر فوق الارتباط **تنشيط** في نافذة إخطارKaspersky PURE التي تظهر في منطقة الإخطارات بشريط المهام.
- في الجزء السفلي من نافذة التطبيق الرئيسية، انقر فوق ارتباط **الترخيص**. في النافذة **التراخيص** التي ستفتح، انقر فوق زر **تنشيط التطبيق**.

عند العمل مع معالج تنشيط التطبيق، ينبغي أن تحدد القيم الخاصة بمجموعة من الإعدادات.

الخطوة 1. إدخال رمز التنشيط

أدخل رمز التنشيط (راجع القسم "طيشنتلا زمر لوح" على الصفحة 28) في الحقل المقابل وانقر فوق زر **التالي**.

الخطوة 2. طلب التنشيط

في حالة إرسال طلب التنشيط بنجاح، سيقوم المعالج بالمتابعة التلقائية إلى الخطوة التالية.

الخطوة 3. إدخال بيانات التسجيل

يُسمح للمستخدمين السجلين باستخدام المزايا التالية:

- إرسال الطلبات إلى خدمة الدعم الفني ومعمل مكافحة الفيروسات من حسابي في Kaspersky على موقع الويب الخاص بشركة Kaspersky Lab.
- إدارة رموز التنشيط.
- تلقي معلومات حول المنتجات الجديدة والعروض الخاصة من Kaspersky Lab.

حدد تفاصيل التسجيل الخاصة بك، وانقر فوق زر **التالي**.

الخطوة 4. تنشيط التطبيق

في حالة نجاح تنشيط التطبيق، سيقوم المعالج بالمتابعة التلقائية إلى النافذة التالية.

الخطوة 5. اكتمال المعالج

تعرض نافذة المعالج هذه معلومات حول نتائج التنشيط.

انقر الزر **إنهاء** لإغلاق المعالج.

شراء ترخيص وتجديده

إذا قمت بتثبيت Kaspersky PURE دون ترخيص تجاري، فيمكنك شراء واحد بعد التثبيت. عند الحصول على ترخيص تجاري، ستتلقى رمزًا للتفعيل يجب عليك استخدامه من أجل تفعيل التطبيق (راجع القسم "تفعيل التطبيق" على الصفحة 31).

وعندما ينتهي ترخيصك، يمكنك تجديده. يمكنك القيام بذلك من خلال تحديد رمز تنشيط جديد دون الانتظار حتى تنتهي صلاحية الترخيص الحالي. عند انتهاء صلاحية الترخيص الحالي، يتم بشكل تلقائي تنشيطKaspersky PURE من خلال رمز التنشيط الاحتياطي.

لشراء ترخيص:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **الترخيص** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة **الترخيص**.
3. في النافذة التي ستفتح، انقر فوق زر **شراء رمز التنشيط**.

سيتم فتح صفحة ويب eStore التي يمكنك من خلالها شراء الترخيص.

لإدخال رمز تنشيط جديد:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **الترخيص** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة **الترخيص**.
3. في النافذة التي يتم فتحها، انقر فوق زر **تنشيط التطبيق**.

ستم فتح "معالج تنشيط التطبيق".

4. أدخل رمز التنشيط في الحقول المقابلة وانقر فوق زر **التالي**.

سيقوم Kaspersky PURE بإرسال البيانات إلى خادم التنشيط للتحقق من صحتها. في حالة نجاح عملية التحقق، يتابع معالج التنشيط تلقائيًا إلى الخطوة التالية.

5. بعد انتهاء تسلسل المعالج، انقر فوق زر **إنهاء**.

إدارة إخطارات التطبيق

تبلغك الإخطارات التي تظهر في منطقة الإخطار بشريط المهام بالأحداث التي تقع في تشغيل التطبيق والتي تستدعي اهتمامك. ووفقًا لدرجة حرج الحدث، قد تتلقى الأنواع التالية من الإخطارات:

- *إخطارات حرجة* – تخبرك بأحداث ذات أهمية بالغة لأمان الكمبيوتر، مثل اكتشاف كائن خبيث أو نشاط خطر في النظام. نوافذ الإخطارات الحرجة والرسائل المنبثقة حمراء اللون.
- *إخطارات مهمة* – تخبرك بأحداث قد تكون مهمة لأمان الكمبيوتر، مثل اكتشاف كائن محتمل إصابته أو نشاط مشكوك فيه بالنظام. نوافذ الإخطارات الهامة والرسائل المنبثقة صفراء اللون.
- *إخطارات معلومات* – تخبرك بأحداث لا تمثل أهمية بالغة لأمان الكمبيوتر. نوافذ الإخطارات المعلوماتية والرسائل المنبثقة خضراء اللون.

في حالة عرض إخطار على الشاشة، ينبغي عليك اختيار أحد الخيارات التي يوفرها الإخطار. الخيار المثالي هو الموصى به كالخيار الافتراضي من قِبل خبراء Kaspersky Lab.

تقييم حالة حماية الكمبيوتر وحل مشكلات الأمان

يتم تمييز المشكلات التي تتعلق بحماية الكمبيوتر بلون النافذة الرئيسية لبرنامج Kaspersky PURE (راجع الشكل الموجود ادناه). ويتغير لون المؤشر اعتمادًا على حالة حماية المضيف: المؤشر الأخضر يعني أن الكمبيوتر محمي؛ والأصفر يعني وجود مشكلات تتعلق بالحماية، والأحمر يعني وجود تهديد خطير على أمان الكمبيوتر. ويوصى بحل مشكلات الأمان وإبطال التهديدات في الحال.

الشكل *1*. مؤشر اللون الأحمر للنافذة الرئيسية

يظهر الزر **إصلاح** (راجع الشكل الموجود أدناه)على مؤشر حالة الحماية في الجزء العلوي الأيسر من نافذة التطبيق الرئيسية عندما يتعرض أمان الكمبيوتر لمشاكل. يؤدي النقر فوق الزر **إصلاح** إلى فتح النافذة **مشكلات الأمان** (راجع الشكل أدناه)، والتي تحتوي على معلومات تفصيلية حول حالة حماية الكمبيوتر، وطرق حل مشكلات الأمان، وإبطال التهديدات.

الشكل 2. نافذة مشكلات الأمان

يتم تجميع المشكلات المرتبطة بالحماية في فئات. لكل مشكلة، يتم سرد الإجراءات التي يمكن استخدامها لحل المشكلة.

يمكنك استخدام التحكم في الشبكة المنزلية للتحقق من حالة الحماية على أجهزة الكمبيوتر الأخرى الموجودة على الشبكة المنزلية (راجع القسم "دعب نع ةيلزنملا ةكبشلا رتويبمك ةزهجأ ةيامح ةرادإ" في الصفحة 44).

تحديث قواعد البيانات والوحدات النمطية للتطبيق

بشكل افتراضي، يقوم Kaspersky PURE بالبحث عن التحديثات تلقائيًا على خوادم تحديث Kaspersky Lab. إذا كان الخادم يخزن مجموعة من التحديثات الحديثة، فسيقومKaspersky PURE بتنزيلها وتثبيتها في وضع الخلفية. يمنك تشغيل تحديث Kaspersky PURE يدويًا في أي وقت من نافذة التطبيق الرئيسية أو من قائمة سياق رمز التطبيق الموجود في منطقة إخطارات شريط المهام.

يجب توفر اتصال بالإنترنت لتنزيل التحديثات من خوادمKaspersky Lab.

لتشغيل تحديث من قائمة السياق الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام،

من قائمة سياق رمز التطبيق، حدد العنصر **تحديث**.

لتشغيل تحديث من نافذة لتطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **تحديث** في القسم **حماية الكمبيوتر** لتشغيل تحديث قاعدة البيانات.

فحص المناطق الحرجة في الكمبيوتر الخاص بك للبحث عن الفيروسات

يتضمن فحص المناطق الحرجة فحص الكائنات التالية:

- الكائنات المحملة عند بدء تشغيل النظام
- ذاكرة النظام
- مقاطع التشغيل بالقرص.

لبدء إجراء فحص للمناطق الحرجة من النافذة الرئيسية للتطبيق:

1. افتح نافذة التطبيق الرئيسية، وانقر الزر **حماية جهاز الكمبيوتر**.
2. في الجزء الأيمن من النافذة التي ستفتح، حدد القسم **الفحص**.
3. في قسم **فحص المناطق الحرجة** الموجودة في الجزء الأيسر من النافذة، انقر فوق زر .

فحص كامل للكمبيوتر للبحث عن الفيروسات

أثناء الفحص الكامل، يقوم Kaspersky PURE بفحص الكائنات التالية بشكل افتراضي:

- ذاكرة النظام؛
- الكائنات المحملة عند بدء تشغيل النظام
- النسخ الاحتياطي للنظام
- محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة.

نوصي بتشغيل فحص كامل بشكل فوري بعد تثبيت Kaspersky PURE على الكمبيوتر.

لبدء تشغيل الفحص الكامل من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **فحص** في القسم **حماية الكمبيوتر** لفتح قائمة مهام الفحص.
3. انقر فوق الارتباط **فحص كامل** لتشغيل الفحص الكامل.

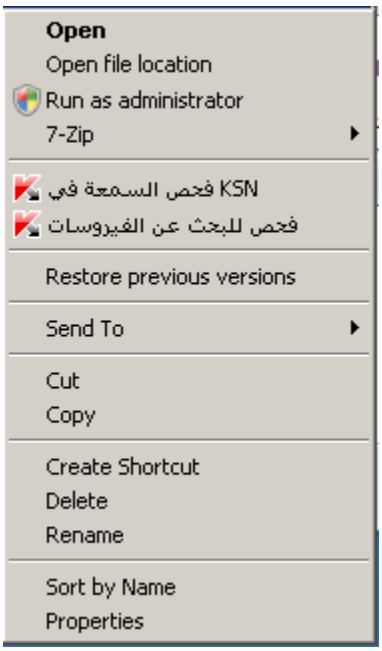
فحص ملف أو مجلد أو قرص أو أي كائن آخر بحثًا عن الفيروسات

يمكنك استخدام الطرق التالية لفحص كائن للبحث عن الفيروسات:

- من قائمة السياق الخاصة بالكائن؛
- من النافذة الرئيسية للتطبيق

لبدء مهمة فحص الفيروسات من قائمة السياق الخاصة بالكائن:

1. افتح نافذة Microsoft Windows Explorer وانتقل إلى المجلد الذي يحتوي على الكائن المراد فحصه.
2. انقر بزر الماوس الأيمن لفتح قائمة السياق الخاصة بالكائن (انظر الشكل أدناه) وحدد **فحص للبحث عن الفيروسات**.



الشكل 3. قائمة السياق للملف القابل للتنفيذ

لبدء فحص كائن من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية، وانقر الزر **حماية جهاز الكمبيوتر**.
2. في الجزء الأيمن من النافذة التي ستفتح، حدد القسم **الفحص**.
3. حدد الكائن المطلوب فحصه باستخدام إحدى الطرق التالية:

- انقر فوق الارتباط **تحديد** الموجود في الجزء الأيسر السفلي من النافذة لفتح النافذة **فحص مخصص** وحدد خانات الاختيار المقابلة للمجلدات والأقراص التي يجب فحصها.

في حالة عدم سرد النافذة لكائن يحتاج للفحص، قم بتنفيذ التالي:

a. انقر فوق الارتباط **إضافة** في الجزء الأيمن السفلي من النافذة ليتم فتح النافذة **حدد كائن للفحص**.

b. في النافذة **تحديد كائن للفحص** التي ستفتح، حدد كائن مطلوب فحصه.

- اسحب كائن لفحصه في المنطقة المخصصة من النافذة الرئيسية (انظر الشكل أدناه).

الشكل *4*. منطقة في النافذة فحص**، يتم سحب الكائن إليها لفحصه**

فحص الكمبيوتر بحثًا عن الثغرات الأمنية

النقاط القابلة للاختراق هي أجزاء غير محمية من رمز برنامج قد يستخدمها الدخلاء عمدًا في أغراض تخصهم مثل نسخ البيانات المستخدمة في التطبيقات غير المحمية. ويساعد فحص الكمبيوتر للبحث عن النقاط القابلة للاختراق في اكتشاف أي نقاط ضعف من هذا القبيل في الكمبيوتر. وينصح بالتخلص من النقاط القابلة للاختراق التي تم اكتشافها.

لبدء تشغيل فحص الثغرات الأمنية من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية، وانقر الزر **حماية جهاز الكمبيوتر**.
2. في الجزء الأيمن من النافذة التي ستفتح، حدد القسم **الفحص**.
3. في النافذة التي يتم فتحها بقسم **فحص نقاط الضعف**، انقر فوق زر .

استعادة ملف تم حذفه أو تنظيفه بواسطة التطبيق

توصي شركة Kaspersky Lab المستخدم بتجنب استعادة الملفات التي تم حذفها وتنظيفها حيث إنها يمكن أن تشكل تهديدًا على جهاز الكمبيوتر.

لاستعادة ملف تم حذفه أو تنظيفه، يمكنك استخدام النسخة الاحتياطية الخاصة به التي تم إنشاؤها بواسطة التطبيق أثناء فحص الملف.

لاستعادة ملف تم حذفه أو تنظيفه بواسطة التطبيق:

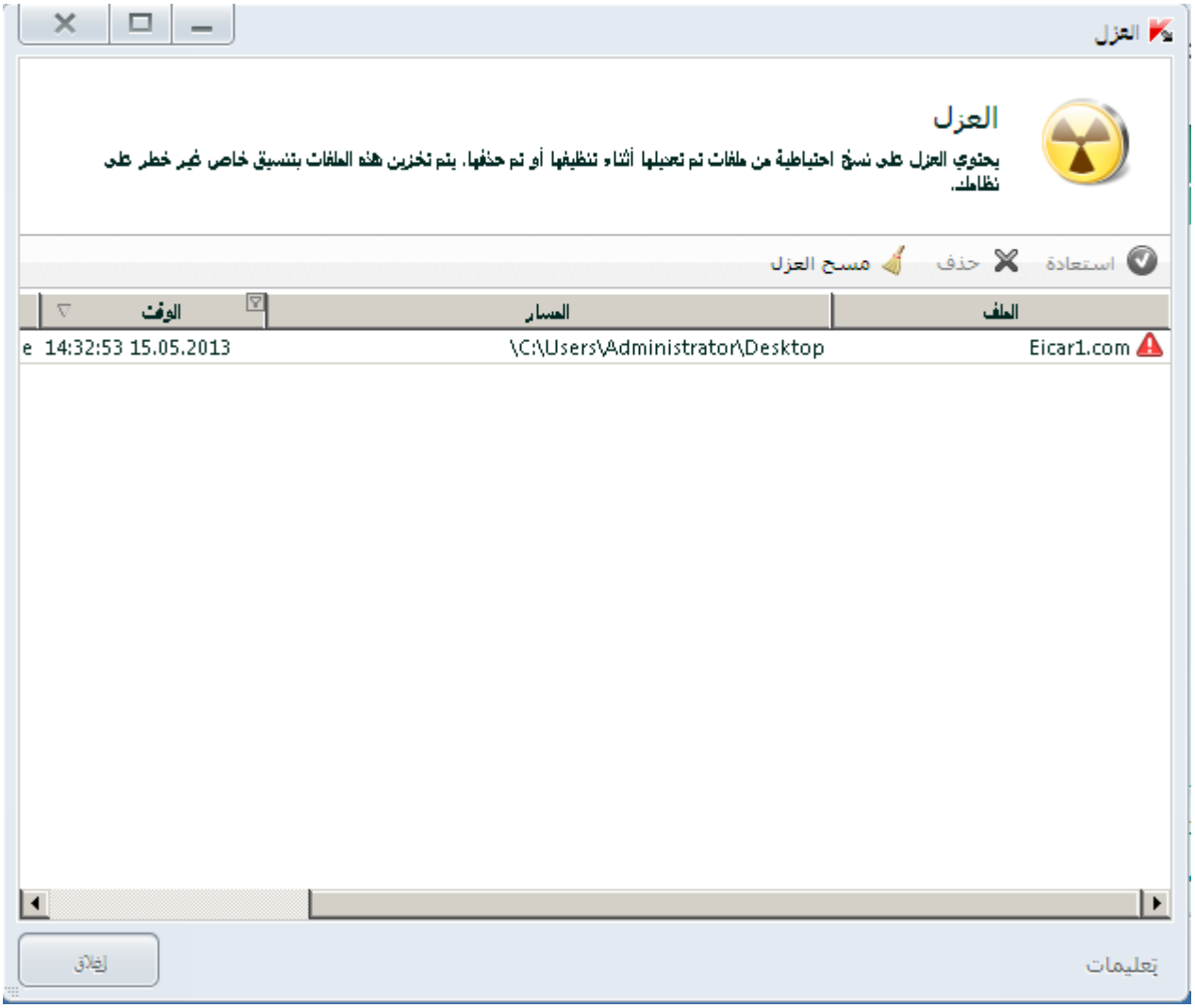
1. افتح نافذة التطبيق الرئيسية، وانقر الزر **حماية جهاز الكمبيوتر**.

2. في الجزء الأيسر من النافذة التي سيتم فتحها، انقر فوق **العزل:** الارتباط <**عدد الملفات**> (انظر الشكل أدناه).

الشكل 5. نافذة حماية الكمبيوتر

3. في نافذة **العزل** التي يتم فتحها، حدد الملف المطلوب من القائمة، وانقر فوق زر **استعادة** (انظر الشكل أدناه).

يقوم Kaspersky PURE باستعادة الملف المحدد إلى المجلد المستخدم لتخزين الملف الذي تمت إزالته وتنظيفه بواسطة التطبيق.



الشكل 6. نافذة العزل

استعادة نظام التشغيل بعد الإصابة

إذا كان يساورك الشك بشأن تلف نظام التشغيل الخاص بالكمبيوتر أو تعديله نتيجة نشاط برمجيات خبيثة أو عطل في النظام، فاستخدم *معالج استكشاف أخطاء Microsoft Windows وإصلاحها بعد الإصابة* الذي يمسح النظام من أي آثار للكائنات خبيثة. وتوصي شركة Kaspersky Lab المستخدم بتشغيل المعالج بعد أن يتم تنظيف الكمبيوتر، وذلك للتأكد من التخلص من جميع التهديدات وإصلاح الضرر الناجم عن الإصابة.

يتحقق المعالج مما إذا كان هناك أي تغييرات في النظام، مثل ما يلي: منع الوصول إلى الشبكة، تغيير امتدادات تنسيقات الملفات المعروفة، تأمين شريط الأدوات، وما إلى ذلك. وتوجد أسباب محتلفة لهذه الأنواع من الأضرار. وقد تتضمن هذه الأسباب نشاط برامج خبيثة، أو تكوين النظام بشكل خاطئ، أو تعطل النظام، أو حتى تشغيل تطبيقات تحسين فعالية النظام بشكل خاطئ.

بعد انتهاء الاستعراض، يقوم المعالج بتحليل المعلومات لتقييم ما إذا كان هناك خلل بالنظام يتطلب سرعة الاهتمام به أم لا. واستناداً إلى الاستعراض، يتم إنشاء قائمة بالإجراءات اللازم تنفيذها للتخلص من المشكلات. ويقوم المعالج بتصنيف هذه الإجراءات إلى فئات بناءً على درجة خطورة المشكلات المكتشفة.

لبدء تشغيل معالج استكشاف أخطاء Microsoft Windows وإصلاحها:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، حدد القسم **أدوات إضافية**.
3. في النافذة التي يتم فتحها بقسم **استكشاف مشكلات Microsoft Windows بعد الإصابة وإصلاحها**، انقر فوق زر **تشغيل**.

سيتم فتح النافذة معالج استكشاف أخطاء Microsoft Windows وإصلاحها.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقم بفحص خطوات المعالج بالتفصيل.

الخطوة 1. بدء تشغيل استكشاف أخطاء Microsoft Windows وإصلاحها

تأكد من تحديد خيار المعالج **البحث عن المشكلات الناتجة عن نشاط البرامج الضارة** وانقر الزر **التالي**.

الخطوة 2. البحث عن المشكلات

سوف يبحث المعالج عن المشكلات والأضرار التي يجب معالجتها. وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 3. تحديد إجراءات استكشاف الأخطاء وإصلاحها

يتم تصنيف جميع الأضرار التي عُثر عليها أثناء الخطوة السابقة وفقاً لنوع الخطر الذي تشكله. وبالنسبة لكل مجموعة من الأضرار، توصي شركة Kaspersky Lab باتخاذ سلسلة من الإجراءات لإصلاح تلك الأضرار. وتوجد ثلاث مجموعات من الإجراءات:

- *إجراءات موصى بها بشدة* وهي الإجراءات التي تقضي على المشكلات التي تمثل خطراً شديداً على الأمان. ننصحك بتنفيذ كافة إجراءات هذه المجموعة.
- *إجراءات مستحسنة* وهي الإجراءات التي تقضي على المشكلات التي تمثل تهديدًا محتملاً. ننصحك بتنفيذ كافة إجراءات هذه المجموعة أيضًا.
- *إجراءات إضافية* وهي الإجراءات التي تقوم بإصلاح تلف النظام الذي لا يمثل تهديداً حالياً، إلا أنه قد يمثل خطراً على أمان الكمبيوتر في المستقبل.

لعرض الإجراءات داخل أي مجموعة، انقر الرمز + الموجود على يمين اسم المجموعة.

لجعل المعالج يقوم بتنفيذ إجراء معين، حدد خانة الاختيار الموجودة على يمين وصف الإجراء المعني. وافتراضيًا، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا لم ترغب في تنفيذ إجراء معين، قم بإلغاء تحديد المربع المجاور له.

يوصى بشدة بإلغاء تحديد خانات الاختيار المحددة افتراضيًا لأن القيام بذلك سوف يجعل الكمبيوتر عرضة للتهديدات.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر فوق زر **التالي**.

الخطوة 4. التخلص من المشكلات

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. وقد يستغرق التخلص من المشكلات بعض الوقت. وبمجرد أن ينتهي استكشاف الأخطاء وإصلاحها، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 5. اكتمال المعالج

انقر الزر **إنهاء** لإغلاق المعالج.

منع البريد الإلكتروني غير المرغوب به (البريد العشوائي)

إذا كنت تتلقى كميات كبيرة من البريد الإلكتروني غير المرغوب فيه (العشوائي)، قم بتمكين مكون مكافحة البريد غير المرغوب فيه وتحديد مستوى الأمن المستحسن.

لتمكين مكافحة البريد الإلكتروني غير المرغوب فيه وتحديد مستوى الأمان المستحسن:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في الجزء الأيمن من النافذة، في القسم **الحماية**، حدد المكون **مكافحة البريد الإلكتروني غير المرغوب فيه**.
4. قم بتحديد الخانة الاختيار **تمكين مكافحة البريد الإلكتروني غير المرغوب فيه** في الجزء الأيسر من النافذة.
5. تأكد من أن مستوى الأمان في القسم **مستوى الأمان** قد تم تعيينه إلى **مستحسن**.

إذا تم تعيين مستوى الأمان على **منخفض** أو **مخصص**, فانقر فوق زر **افتراضي**. سيتم تعيين مستوى الأمان تلقائيًا على **مستحسن**.

فحص البريد الإلكتروني وتصفية مرفقات رسائل البريد الإلكتروني

يتيح برنامج Kaspersky PURE فحص رسائل البريد الإلكتروني لاكتشاف الكائنات الخطرة باستخدام مكون مكافحة فيروسات البريد. يبدأ تشغيل مكون مكافحة فيروسات البريد عند بدء تشغيل نظام التشغيل ويبقى في ذاكرة الوصول العشوائي (RAM) بشكل دائم ليقوم بفحص كل رسائل البريد الإلكتروني التي يتم إرسالها أو تلقيها عبر بروتوكولات POP3، وSMTP، وIMAP، وMAPI، وNNTP، إلى جانب الاتصالات المشفرة (SSL) عبر بروتوكولات POP3، وSMTP، وIMAP.

بشكل افتراضي، يفحص مكون مكافحة فيروسات البريد كلاً من البريد الإلكتروني الوارد والصادر. يمكنك تمكين فحص البريد الوارد فقط إذا لزم الأمر.

لفحص رسائل البريد الإلكتروني الوارد فقط:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في الجزء الأيمن من النافذة، في القسم **مركز الحماية**، حدد المكون **مكافحة فيروسات البريد**.
4. انقر الزر **الإعدادات** في الجزء الأيسر من النافذة.

يتم فتح نافذة **مكافحة فيروسات البريد**.

5. في النافذة التي سيتم فتحها، استخدم علامة التبويب **عام** الموجودة في القسم **نطاق الحماية** لتحديد الخيار **الرسائل الواردة فقط**.

في حالة عدم اكتشاف أي تهديدات في رسالة البريد الإلكتروني، أو في حالة تنظيف كل الكائنات المصابة بنجاح، تصبح الرسالة متاحة للعمليات الأخرى. إذا فشل مكون مكافحة فيروسات البريد في تنظيف كائن مصاب، فإنه يقوم بإعادة تسمية الكائن أو حذفه من الرسالة وتوسعة عنوان الرسالة ليتضمن إخطارًا بأنه تمت معالجة الرسالة بواسطة Kaspersky PURE. قبل حذف أي كائن، يقوم برنامج Kaspersky PURE بإنشاء نسخة احتياطية منه ووضعها في العزل.

قد تنتشر البرامج الخبيثة في شكل مرفقات برسائل البريد الإلكتروني. يمكنك تمكين تصفية المرفقات في رسائل البريد الإلكتروني. تتيح التصفية إعادة تسمية الملفات المرفقة من الأنواع التي تحددها أو حذفها تلقائيًا.

لتمكين تصفية المرفقات في رسائل البريد الإلكتروني:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في الجزء الأيمن من النافذة، في القسم **مركز الحماية**، حدد المكون **مكافحة فيروسات البريد**.
4. انقر الزر **الإعدادات** في الجزء الأيسر من النافذة.

   يتم فتح نافذة **مكافحة فيروسات البريد**.
5. في علامة التبويب **عامل تصفية المرفقات** بالنافذة التي يتم فتحها، حدد وضع تصفية المرفقات (**إعادة تسمية أنواع المرفقات المحددة** أو **حذف أنواع المرفقات المحددة**).
6. من قائمة أنواع الملفات (الامتدادات)، حدد أنواع المرفقات التي ينبغي تصفيتها.

   إذا كنت تريد إضافة قناع نوع ملف جديد:

   a. انقر فوق الارتباط **إضافة** في الجزء السفلي من النافذة لفتح النافذة **إدخال قناع لاسم ملف**.

   b. في النافذة التي يتم فتحها، أدخل قناعًا لنوع الملف.
7. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

تقييم الحالة الآمنة لموقع الويب

يسمح Kaspersky PURE بفحص موقع الويب لضمان أمانه قبل الانتقال إلى موقع الويب بواسطة ارتباط. لتنفيذ هذا الأمر، يتم استخدام وحدة نمطية يطلق عليها مستشار *Kaspersky* لعناوين مواقع الويب.

مستشار Kaspersky لعناوين URL غير متاح في Microsoft Internet Explorer 10 من نمط Metro، إلى جانب Microsoft Internet Explorer 10 في حالة تحديد خانة الاختيار **الوضع المحمي المحسّن** في إعدادات المستعرض.

يكون مستشار Kaspersky لعناوين URL متكاملاً في مستعرضات Microsoft Internet Explorer وGoogle Chrome™ و Mozilla™ Firefox™، ويقوم بفحص الارتباطات الموجودة على صفحات الويب المفتوحة في المستعرض. يعرض Kaspersky PURE أحد الرموز التالية بجوار كل ارتباط:

- – إذا كانت صفحة الويب التي تم فتحها عن طريق النقر فوق الارتباط آمنة وفقًا لـ Kaspersky Lab
- – إذا لم تكن هناك معلومات حول حالة سلامة صفحة الويب التي تم فتحها عن طريق النقر فوق الارتباط
- – إذا كانت صفحة الويب التي تم فتحها عن طريق النقر فوق الارتباط خطيرة وفقًا لـ Kaspersky Lab

عند تمرير الماوس فوق الرمز، يتم عرض نافذة منبثقة تتضمن الكثير من التفاصيل حول الارتباط المعروض.

بشكل افتراضي، يقوم Kaspersky PURE بفحص الارتباطات الموجودة في نتائج البحث فقط. يمكنك تمكين فحص الارتباط على كل موقع ويب.

لتمكين فحص الارتباط على كل موقع ويب:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في النافذة **إعدادات** التي سيتم فتحها، انتقل إلى القسم **مركز الحماية** وحدد القسم الفرعي **مكافحة فيروسات الويب** وانقر فوق زر **إعدادات**.

   سيتم فتح النافذة **مكافحة فيروسات الويب**.
4. في النافذة التي يتم فتحها، من علامة التبويب **التصفح الآمن** في قسم **مستشار Kaspersky لعناوين URL**، انقر فوق زر **الإعدادات**.

   سيتم فتح النافذة **إعدادات مستشار Kaspersky لعناوين مواقع الويب**.
5. في النافذة التي سيتم فتحها، في القسم **وضع الفحص** حدد **كل عناوين مواقع الويب**.
6. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

منع الوصول إلى مواقع الويب الخاصة بالمناطق المختلفة

وفقًا للإحصائيات التي تم تجميعها بواسطة Kaspersky Lab، قد تختلف معدلات إصابة مواقع الويب اعتمادًا على دولة المنشأ. يستخدم Kaspersky PURE مكونًا يُعرف باسم عامل التصفية الجغرافية لمنع الوصول إلى مواقع الويب التي تنتمي إلى المجالات الإقليمية المصنفة على أنها ذات معدلات إصابة مرتفعة.

عندما يتم تمكين عامل التصفية الجغرافية، يقوم Kaspersky PURE بالسماح بالوصول إلى المجال الإقليمي، أو منع الوصول إليه، أو المطالبة بالحصول على إذن وصول منك، اعتمادًا على الاختيار الذي تحدده أنت.

لتمكين عامل التصفية الجغرافي وتكوينه:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في النافذة **إعدادات** التي سيتم فتحها، انتقل إلى القسم **مركز الحماية** وحدد القسم الفرعي **مكافحة فيروسات الويب** وانقر فوق زر **إعدادات**.

   سيتم فتح النافذة **مكافحة فيروسات الويب**.
4. في النافذة التي سيتم فتحها، على علامة التبويب **عامل التصفية الجغرافي**، حدد خانة الاختيار **تمكين التصفية حسب المجالات الإقليمية**.
5. في الجزء السفلي من النافذة، في القائمة الخاصة بالمجالات التي يتم التحكم بها، حدد المجالات التي يجب أن يتم السماح بالوصول إليها أو منع الوصول إليها أو حدد المجالات التي تتطلب طلب الحصول على إذن للوصول إليها.
6. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

إدارة حماية الشبكة المنزلية عن بُعد

تم تصميم وظائف التحكم في الشبكة المنزلية للتحكم في Kaspersky PURE المثبت على أجهزة كمبيوتر الشبكة المنزلية عن بعد من محطة عمل المسؤول.

يسمح لك التحكم في الشبكة المنزلية بتحقيق مهام الأمان التالية الخاصة بالشبكة المنزلية:

- عرض قائمة تضم مشاكل الأمان على كمبيوتر منفصل على الشبكة وإصلاح بعضها عن بُعد
- تشغيل عمليات فحص للبحث عن الفيروسات على أجهزة كمبيوتر متعددة على الشبكة المنزلية في نفس الوقت
- تحديث قواعد البيانات الموجودة على أجهزة كمبيوتر متعددة على الشبكة المنزلية في نفس الوقت

لعرض قائمة مشكلات الأمان على كمبيوتر محدد على الشبكة:

1. افتح نافذة التطبيق الرئيسية وانقر الزر **التحكم في الشبكة المنزلية** في الجزء السفلي من النافذة.
2. في الجزء العلوي من النافذة **التحكم في الشبكة المنزلية** التي ستفتح، حدد الكمبيوتر الذي تريد عرض قائمة المشكلات الخاصة به، وانتقل إلى القسم **المعلومات**.
3. في الجزء الأيسر من النافذة بقسم **المشاكل**، انقر فوق زر **القائمة**.

يتم فتح نافذة **مشاكل الأمان** مع عرض معلومات حول مشاكل الأمان التي تم اكتشافها على الكمبيوتر المحدد.

لفحص أجهزة كمبيوتر متعددة على الشبكة للبحث عن الفيروسات:

1. افتح نافذة التطبيق الرئيسية وانقر الزر **التحكم في الشبكة المنزلية** في الجزء السفلي من النافذة.

   سيتم فتح النافذة **التحكم في الشبكة المنزلية**.
2. انقر فوق الارتباط **الفحص للبحث عن الفيروسات** لفتح النافذة **التشغيل المجمع للفحص**.
3. في النافذة **التشغيل المجمع للفحص**، حدد علامة التبويب التي تحتوي على نوع الفحص المطلوب (**فحص كامل** أو **فحص المناطق الحرجة**).
4. حدد أجهزة الكمبيوتر التي ترغب في فحصها وانقر فوق زر **تشغيل الفحص**.

لتحديث قواعد البيانات على أجهزة كمبيوتر شبكة متعددة في نفس الوقت:

1. افتح نافذة التطبيق الرئيسية وانقر الزر **التحكم في الشبكة المنزلية** في الجزء السفلي من النافذة.

   سيتم فتح النافذة **التحكم في الشبكة المنزلية**.
2. انقر فوق الارتباط **تحديث قواعد البيانات** لفتح النافذة **التشغيل المجمع للفحص**.
3. في النافذة **التشغيل المجمع للفحص**، حدد أجهزة الكمبيوتر التي ترغب في تحديث قواعد البيانات عليها وانقر فوق زر **تشغيل التحديث**.

التعامل مع التطبيقات غير المعروفة

يساعد Kaspersky PURE على تقليل خطر الاشتراك في استخدام تطبيقات غير معروفة (مثل خطر الإصابة بالفيروسات والتغييرات غير المرغوبة في إعدادات نظام التشغيل).

يتضمن Kaspersky PURE مكونات وأدوات لفحص سمعة التطبيق وبدء تشغيله في وضع التشغيل الآمن، الذي يعزله من نظام التشغيل.

التحكم في أنشطة التطبيقات الموجودة على الكمبيوتر والشبكة

يمنع التحكم في التطبيق التطبيقات من تنفيذ الإجراءات التي قد تكون خطرة على النظام، ويضمن التحكم في الوصول إلى موارد نظام التشغيل وبيانات الهوية.

يقوم المكون بتتبع الإجراءات في النظام التي تنفذها التطبيقات المثبتة على الكمبيوتر، كما يقوم بتنظيمها وفقًا لقواعد التحكم في التطبيق. تنظم هذه القواعد النشاط الذي يؤثر على أمان الكمبيوتر، بما في ذلك وصول التطبيق إلى الموارد المحمية، مثل الملفات والمجلدات، ومفاتيح التسجيل، وعناوين شبكة الاتصال.

يتم التحكم في نشاط التطبيق وفقًا مكون جدار الحماية.

عندما يتم تشغيل النظام لأول مرة على الكمبيوتر، يقوم مكون التحكم في التطبيق بفحص سلامته والنقل إلى إحدى المجموعات (موثوق به أو غير موثوق به أوعالي التقييد أو منخفض التقييد). تقوم المجموعة بتعريف القواعد التي ينبغي على برنامج Kaspersky PURE تطبيقها للتحكم في نشاط هذا التطبيق.

يمكنك تحرير قواعد التحكم في التطبيق يدويًا.

لتحرير قواعد التحكم في التطبيق يدويًا:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في النافذة **الإعدادات** التي سيتم فتحها، حدد القسم الفرعي **التحكم في التطبيق** في **مركز الحماية**.
4. في الجزء الأيسر من النافذة، في القسم **تكوين قواعد التطبيق وحماية بيانات الهوية الرقمية والموارد المحمية**، انقر فوق زر **التطبيقات**.
5. في النافذة **التطبيقات** التي ستفتح، حدد التطبيق المطلوب من القائمة ثم انقر فوق زر **تحرير**.
6. في النافذة **قواعد التطبيق** التي ستفتح، قم بتعيين قواعد التطبيق.

- لتكوين قواعد الوصول إلى موارد نظام التشغيل لأحد التطبيقات:
  a. من علامة التبويب **تسجيل النظام والملفات** حدد فئة المورد المطلوبة.
  b. انقر بزر الماوس الأيمن فوق العمود الذي يتضمن إجراء متوفر على المورد (**قراءة** أو **كتابة** أو **حذف** أو **إنشاء**) لفتح قائمة سياق وحدد القيمة المطلوبة منه (**السماح** أو **المنع** أو **المطالبة بتنفيذ إجراء**).
- لتكوين حقوق التطبيق لتنفيذ إجراءات مختلفة في نظام التشغيل:
  a. من علامة التبويب **الحقوق** حدد فئة الحقوق المطلوبة.
  b. انقر بزر الماوس الأيمن فوق العمود **الإذن** لفتح قائمة السياق وتحديد القيمة المطلوبة منها (**السماح** أو **المنع** أو **المطالبة بإجراء**).
- لتكوين حقوق التطبيق لتنفيذ إجراءات مختلفة على الشبكة:
  a. من علامة التبويب **قواعد الشبكة**، انقر فوق زر **إضافة**.

ستفتح النافذة **قاعدة الشبكة**.

b. في النافذة التي ستفتح، حدد إعدادات القاعدة المطلوبة وانقر فوق زر **موافق**.

c. قم بتعيين أولوية للقاعدة الجديد عن طريق استخدام الزرين **تحريك لأعلى** و**تحريك لأسفل** للانتقال لأعلى القائمة وأسفلها.

- لاستبعاد إجراءات محددة من نطاق التحكم في التطبيق، من علامة التبويب **الاستثناءات** حدد خانات الاختيار الخاصة بالإجراءات التي يجب عدم التحكم فيها.

بالنسبة إلى كافة الاستثناءات التي تم إنشاؤها في القواعد لتطبيقات المستخدم، يمكن الوصول إليها في نافذة إعدادات التطبيق في القسم **التهديدات والاستثناءات**.

7. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

فحص سمعة التطبيق

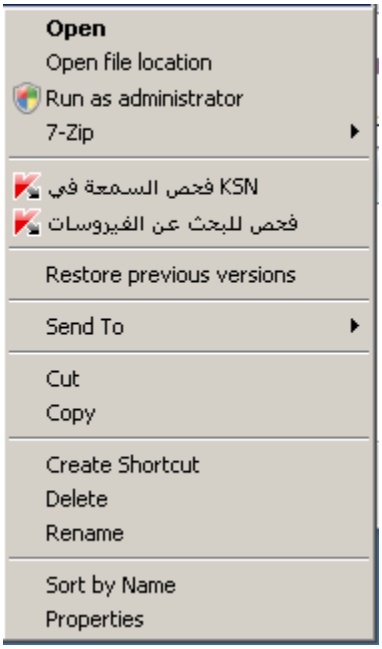
يتيح لك Kaspersky PURE معرفة سمعة التطبيقات من المستخدمين من جميع أرجاء العالم. وتتضمن سمعة التطبيق المؤشرات التالية:

- اسم الناشر؛
- معلومات حول التوقيع الرقمي (تكون متاحة في حالة وجود توقيع رقمي)؛
- معلومات حول المجموعة التي تم تضمين التطبيق بها بواسطة التحكم في التطبيق أو بواسطة معظم مستخدمي شبكة أمان Kaspersky؛
- عدد مستخدمي شبكة أمان Kaspersky الذين يستخدمون التطبيق (يتوفر في حالة أن التطبيق ينتمي إلى مجموعة موثوقة في قاعدة بيانات شبكة أمان Kaspersky)؛
- الوقت الذي يُصبح فيه التطبيق معروفًا في شبكة أمان Kaspersky؛
- البلدان التي ينتشر بها التطبيق.

يتوفر فحص سمعة التطبيق إذا وافقت على المشاركة في شبكة أمان Kaspersky.

لمعرفة سمعة التطبيق،

حدد **فحص السمعة في KSN** في قائمة سياق الملف القابل للتنفيذ (راجع الشكل الموجود أدناه).



الشكل 7. قائمة السياق الخاصة بملف قابل للتنفيذ في *Microsoft Windows*

سيتم فتح نافذة تتضمن معلومات حول سمعة التطبيق في KSN

حماية البيانات الخاصة من السرقة

يساعدك Kaspersky PURE على حماية بياناتك الشخصية من السرقة:

- كلمات المرور وأسماء المستخدمين وبيانات التسجيل الأخرى؛
- أرقام الحساب وبطاقات البنك،
- بيانات سرية.

يشتمل برنامج Kaspersky PURE على مكونات وأدوات تتيح لك حماية بياناتك الشخصية ضد محاولات السرقة التي يقوم بها القراصنة باستخدام طرق مثل الاحتيال واعتراض البيانات المدخلة باستخدام لوحة المفاتيح.

توفر مزايا الخدمات النقدية الآمنة الحماية للبيانات عند استخدام الخدمات البنكية على الإنترنت والتسوق من متاجر الإنترنت.

يتم ضمان الحماية من الاحتيال بواسطة مكون مكافحة الاحتيال، والتي يتم تنفيذها في مكونات مكافحة فيروسات الويب، ومكافحة البريد الإلكتروني غير المرغوب فيه، ومكافحة فيروسات المراسلة الفورية.

توفر لوحة المفاتيح الظاهرية، وإدخال لوحة المفاتيح الآمن، ومدير كلمات المرور الحماية من اعتراض البيانات المدخلة من لوحة المفاتيح.

يتم ضمان حماية البيانات من الوصول غير المصرح به باستخدام تشفير البيانات.

تم تصميم معالج منظف الخصوص لتنظيف الكمبيوتر من كل المعلومات حول أنشطة المستخدم.

في هذا القسم:

الخدمات النقدية الآمنة

لتوفير الحماية للبيانات السرية التي تقوم بإدخالها على مواقع الويب الخاصة بالبنوك وأنظمة السداد (مثل أرقام البطاقات البنكية وكلمات المرور الخاصة بالوصول إلى الخدمات البنكية عبر الإنترنت)، بالإضافة إلى منع سرقة الأصول عند السداد عبر الإنترنت، يوفر لك برنامج Kaspersky PURE خيارًا يمكنك من فتح مواقع الويب هذه في وضع التشغيل الآمن لمواقع الويب.

لا يمكن تشغيل وضع التشغيل الآمن لمواقع الويب في حالة عدم تحديد خانة الاختيار **تمكين الدفاع الذاتي** في قسم **الإعدادات المتقدمة** داخل القسم الفرعي **الدفاع الذاتي** بنافذة إعدادات التطبيق.

يمكنك تكوين الخدمات النقدية الآمنة بحيث يقوم التطبيق بالتعرف التلقائي على مواقع الويب الخاصة بالبنوك وأنظمة السداد.

الخدمات النقدية الآمنة غير متاحة في Microsoft Internet Explorer 10 من نمط Metro، إلى جانب Microsoft Internet Explorer 10 في حالة تحديد خانة الاختيار **الوضع المحمي المحسّن** في إعدادات المستعرض. يمكنك تمكين وضع التشغيل الآمن لمواقع الويب من واجه Kaspersky PURE.

لتكوين الخدمات النقدية الآمنة:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في النافذة **الإعدادات** التي ستفتح، في القسم **مركز الحماية**، حدد القسم الفرعي **الخدمات النقدية الآمنة**.
4. حدد خانة الاختيار **تمكين الخدمات النقدية الآمنة**.
5. لتمكين الإخطارات بنقاط الضعف المكتشفة في نظام التشغيل قبل بدء تشغيل التشغيل الآمن لمواقع الويب، حدد خانة الاختيار **الإخطار بنقاط الضعف الموجودة في نظام التشغيل**.
6. لتكوين الخدمات النقدية الآمنة لموقع ويب محدد:

a. في قائمة **مواقع ويب البنوك وأنظمة السداد** انقر فوق زر **إضافة**.

سيتم فتح النافذة **موقع ويب للخدمات النقدية الآمنة**.

b. في النافذة التي ستفتح، في الحقل **موقع ويب البنك أو نظام السداد** أدخل عنوان URL لموقع الويب التي يجب أن يتم فتحه في وضع التشغيل الآمن لمواقع الويب.

يجب أن يكون اسم موقع الويب مسبوقًا ببادئة بروتوكول https:// التي يستخدمها وضع التشغيل الآمن لمواقع الويب بشكل افتراضي.

c. عند الضرورة، في الحقل **الوصف** أدخل اسم أو وصف موقع الويب هذا.

d. حدد طريقة لبدء التشغيل الآمن لمواقع الويب عند تشغيل موقع الويب:

- إذا كنت تريد أن يعرض عليك Kaspersky PURE بدء وضع التشغيل الآمن لمواقع الويب في كل مرة تقوم فيها بفتح موقع الويب، فحدد **المطالبة باتخاذ إجراء**.
- إذا كنت تريد أن يقوم Kaspersky PURE بفتح موقع ويب في وضع التشغيل الآمن لمواقع الويب بشكل تلقائي، فحدد **تشغيل حماية المستعرض تلقائيًا**.
- إذا كنت تريد تعطيل الخدمات النقدية الآمنة لموقع الويب، فحدد **عدم تشغيل حماية المستعرض**.

7. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

الحماية ضد الاحتيال

يتم توفير الحماية ضد الاحتيال بواسطة وظيفة مكافحة الاحتيال المنفذة في المكون مكافحة فيروسات الويب والمكون مكافحة البريد الإلكتروني غير المرغوب فيه والمكون مكافحة فيروسات المراسلة الفورية. وتمكن هذه المكونات من ضمان توفير حماية شاملة ضد الاحتيال.

يمكنك تكوين إعدادات إضافية للحماية ضد الاحتيال في المكون مكافحة فيروسات الويب والمكون مكافحة فيروسات المراسلة الفورية.

لتكوين الحماية ضد الاحتيال عند تشغيل المكون مكافحة فيروسات الويب:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في النافذة **إعدادات** التي سيتم فتحها، انتقل إلى القسم **الحماية** وحدد القسم الفرعي **مكافحة فيروسات الويب** وانقر فوق زر **إعدادات**.

سيتم فتح النافذة **مكافحة فيروسات الويب**.

4. في النافذة التي يتم فتحها، من علامة التبويب **عام**، في قسم **مستشار Kaspersky لعناوين URL**، حدد خانة الاختيار **التحقق من صفحات الويب للبحث عن الطرق الاحتيالية**.
5. إذا كنت تريد أن يستخدم مكون مكافحة الاحتيال التحليل المساعد على الاكتشاف، فانقر فوق زر **إضافي** عند فحص صفحات الويب.

سيتم فتح النافذة **إعدادات مكافحة الاحتيال**.

6. في النافذة التي يتم فتحها، حدد خانة الاختيار **استخدام التحليل المساعد على الاكتشاف لفحص صفحات ويب ضد الاحتيال**، وقم بتعيين مستوى تفاصيل الفحص.

7. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

لتكوين الحماية ضد الاحتيال للاستخدام أثناء تشغيل مكون مكافحة فيروسات المراسلة الفورية:

1. افتح نافذة التطبيق الرئيسية.

2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.

3. في النافذة **الإعدادات** التي سيتم فتحها، حدد القسم الفرعي **مكافحة فيروسات المراسلة الفورية الحماية**.

4. في الجزء الأيسر من النافذة بقسم **طرق الفحص**، حدد خانة الاختيار **التحقق مما إذا كانت عناوين مواقع الويب مدرجة في قاعدة بيانات عناوين مواقع الويب الاحتيالية**.

5. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

استخدام لوحة المفاتيح الظاهرية

عند العمل على الإنترنت، تحتاج كثيرًا إلى إدخال بياناتك الشخصية أو اسم المستخدم وكلمة المرور خاصتك. على سبيل المثال، يكون هذا الأمر مطلوبًا عند التسجيل في مواقع الويب والتسوق عبر الإنترنت أو استخدام التعاملات البنكية عبر الإنترنت.

هناك خطر من اعتراض هذه المعلومات الشخصية عن طريق معترضي لوحات المفاتيح، أو برامج رصد لوحة المفاتيح، وهي عبارة عن برامج تقوم بتسجيل ضغطات لوحة المفاتيح المادية.

تمنع لوحة المفاتيح الظاهرية اعتراض البيانات المدخلة باستخدام لوحة المفاتيح.

تمنع لوحة المفاتيح الظاهرية فقط اعتراض بيانات الخصوصية فقط عند العمل مع المستعرضات Microsoft Internet Explorer، وMozilla Firefox، و Google Chrome. عند الاستخدام مع مستعرضات أخرى، لا تحمي لوحة المفاتيح الظاهرية البيانات الشخصية التي يتم إدخالها ضد الاستقبال.

لوحة المفاتيح الظاهرية غير متاحة في Microsoft Internet Explorer 10 من نمط Metro، إلى جانب Microsoft Internet Explorer 10 في حالة تحديد خانة الاختيار **الوضع المحمي المحسّن** في إعدادات المستعرض. في هذه الحالة، نوصي باستخدام لوحة المفاتيح الظاهرية من واجهة Kaspersky PURE.

ولا تستطيع لوحة المفاتيح الظاهرية حماية بياناتك الشخصية إذا كان موقع الويب الذي يتطلب توفير هذه البيانات قد تمت مهاجمته، لأنه إذا تم هذا الأمر سيحصل المهاجم على المعلومات مباشرًة.

وتستطيع الكثير من البرامج المصنفة كبرامج تجسس التقاط لقطات للشاشة، والتي يمكن نقلها بشكل تلقائي إلى دخيل لإجراء المزيد من التحليل ولسرقة البيانات الشخصية للمستخدم. تمنع لوحة المفاتيح الظاهرية استخدام لقطات الشاشة لتفسير البيانات الشخصية.

لا تحول لوحة المفاتيح الظاهرية دون أخذ لقطات الشاشة باستخدام مفتاح **Print Screen** والمجموعات الأخرى من المفاتيح التي توفرها إعدادات نظام التشغيل، وكذلك أخذ لقطات الشاشة باستخدام DirectX.

ميزات لوحة المفاتيح الظاهرية:

- يجب الضغط على لوحة المفاتيح الظاهريةباستخدام مؤشر الماوس.
- على العكس من لوحة المفاتيح الحقيقية، من المستحيل أن يتم الضغط على مفاتيح متعددة من لوحة المفاتيح الظاهرية في نفس الوقت. لهذا فإن استخدام مجموعات المفاتيح (مثل **ALT+F4**) يتطلب الضغط على المفتاح الأول (على سبيل المثال، **ALT**)، ثم الضغط على المفتاح الثاني (على سبيل المثال، **F4**)، ثم الضغط على المفتاح الأول مرة أخرى. يعتبر الضغط على المفتاح مرة أخرى موازيًا لتحرير المفتاح على لوحة المفاتيح الحقيقية.

- يمكن تبديل لغة لوحة المفاتيح الظاهرية باستخدام بعض الاختصارات المكونة في إعدادات نظام التشغيل الخاص بلوحة المفاتيح الفعلية. يجب النقر بزر الماوس الأيمن فوق المفتاح الآخر (على سبيل المثال، إذا تم تكوين الاختصار **LEFT ALT+SHIFT** في إعدادات نظام التشغيل لتبديل لغة لوحة المفاتيح، يجب النقر بزر الماوس الأيسر فوق المفتاح **LEFT ALT** والنقر بزر الماوس الأيمن فوق المفتاح **SHIFT**).

لضمان حماية البيانات المدخلة من لوحة المفاتيح الظاهرية، ينبغي إعادة تشغيل الكمبيوتر بعد تثبيت Kaspersky PURE.

يمكن فتح لوحة المفاتيح الظاهرية بأي من الطرق التالية:

- من القائمة السياقية الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام؛
- من نافذة التطبيق الرئيسية،
- من نافذة مستعرضات Microsoft Internet Explorer أو Mozilla Firefox أو Google Chrome؛
- باستخدام رمز بدء التشغيل السريع الخاص بلوحة المفاتيح الظاهرية في حقول الإدخال على مواقع الويب؛

يمكنك تكوين عرض رمز بدء التشغيل السريع في حقول الإدخال على مواقع الويب.

- باستخدام مجموعة من المفاتيح في لوحة مفاتيح الكمبيوتر.

لفتح لوحة المفاتيح الظاهرية من قائمة السياق الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام، حدد ***أدوات→لوحة المفاتيح الظاهرية*** *من قائمة السياق الخاصة برمز التطبيق(انظر الشكل أدناه).*

الشكل 8. قائمة السياق الخاصة برمز برنامج *Kaspersky PURE*

لفتح لوحة المفاتيح الظاهرية من نافذة التطبيق الرئيسية:

1. حدد القسم **إدارة كلمات المرور** في الجزء السفلي من نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة التي سيتم فتحها، انقر فوق زر **لوحة المفاتيح الظاهرية**.

لفتح لوحة المفاتيح الظاهرية من نافذة المستعرض،

انقر فوق زر **لوحة المفاتيح الظاهرية** الموجود في شريط أدوات Microsoft Internet Explorer، أو Mozilla Firefox، أو Google Chrome.

لفتح لوحة المفاتيح الظاهرية باستخدام لوحة مفاتيح الكمبيوتر،

اضغط على اختصار لوحة المفاتيح **CTRL + ALT + SHIFT + P**.

لتكوين عرض رمز بدء التشغيل السريع للوحة المفاتيح الظاهرية في حقول الإدخال على مواقع الويب:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في نافذة **الإعدادات** التي يتم فتحها، في قسم **مركز الحماية**، حدد القسم الفرعي **الإدخال الآمن للبيانات**.
4. في الجزء الأيسر من النافذة بقسم **لوحة المفاتيح الظاهرية**، حدد خانة الاختيار **إظهار رمز بدء التشغيل السريع في حقول إدخال البيانات**، وانقر فوق زر **الإعدادات**.

   يتم فتح نافذة **لوحة المفاتيح الظاهرية**.
5. في النافذة التي يتم فتحها، قم بتعيين قواعد عرض رمز بدء التشغيل السريع:

- من علامة تبويب **الفئات**، حدد خانات الاختيار الخاصة بالفئات التي ينبغي عليها عرض رمز بدء التشغيل السريع في حقول الإدخال.
- إذا كنت تريد عرض رمز بدء التشغيل السريع في حقول الإدخال على مواقع الويب التي يتم فتحها في وضع التشغيل الآمن لمواقع الويب عند استخدام الخدمات النقدية الآمنة، من علامة تبويب **الفئات**، حدد خانة الاختيار **إظهار رمز بدء التشغيل السريع للوحة المفاتيح الظاهرية في حقول الخدمات النقدية الآمنة**.
- إذا كنت تريد تمكين عرض رمز بدء التشغيل السريع في حقول الإدخال على موقع ويب معين:

a. من علامة تبويب **الاستثناءات** في قائمة **إظهار رمز بدء التشغيل السريع على مواقع الويب**، انقر فوق زر **إضافة**.

   يتم فتح نافذة **إظهار رمز بدء التشغيل السريع**.

b. في النافذة التي يتم فتحها، أدخل عنوان URL لموقع الويب في حقل **عنوان URL**، وحدد أحد خيارات عرض رمز بدء التشغيل السريع على موقع الويب هذا (**إظهار الرمز فقط على صفحة الويب المحددة** أو **إظهار الرمز على موقع الويب بأكمله**).

6. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

إدخال لوحة المفاتيح الآمن

عند العمل على الإنترنت، تحتاج كثيرًا إلى إدخال بياناتك الشخصية أو اسم المستخدم وكلمة المرور خاصتك. ويحدث هذا، على سبيل المثال، أثناء تسجيل حساب على مواقع الويب، أو أثناء التسوق عبر الويب، أو إجراء معاملات بنكية على الإنترنت.

هناك خطر من اعتراض هذه المعلومات الشخصية عن طريق معترضي لوحات المفاتيح، أو برامج رصد لوحة المفاتيح، وهي عبارة عن برامج تقوم بتسجيل ضغطات لوحة المفاتيح المادية.

تحول وظيفة إدخال لوحة المفاتيح الآمن دون اعتراض البيانات المدخلة باستخدام لوحة المفاتيح.

تكون وظيفة إدخال لوحة المفاتيح الآمن متاحة فقط للمستعرضات Microsoft Internet Explorer، وMozilla Firefox، وGoogle Chrome. عند استخدام مستعرضات الويب الأخرى، لا تتم حماية البيانات المدخلة من لوحة مفاتيح الكمبيوتر من الاعتراض.

حماية إدخال البيانات غير متاحة في Microsoft Internet Explorer 10 من نمط Metro، إلى جانب Microsoft Internet Explorer 10 في حالة تحديد خانة الاختيار **الوضع المحمي المحسّن** في إعدادات المستعرض.

لا تستطيع وظيفة إدخال لوحة المفاتيح الآمن حماية بياناتك الشخصية إذا تعرض موقع الويب - الذي يتطلب إدخال مثل هذه البيانات - للتسلل، حيث سيتم في هذه الحالة توجيه المعلومات مباشرةً إلى الدخلاء.

يمكنك تكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر على مواقع الويب المختلفة. بعد تكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر، ليس عليك اتخاذ أي إجراءات إضافية عند إدخال البيانات.

لحماية البيانات المدخلة من لوحة مفاتيح الكمبيوتر، ينبغي إعادة تشغيل الكمبيوتر بعد تثبيت برنامج Kaspersky PURE.

لتكوين حماية إدخال البيانات من لوحة مفاتيح الكمبيوتر:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في نافذة **الإعدادات** التي يتم فتحها، في قسم **مركز الحماية**، حدد القسم الفرعي **الإدخال الآمن للبيانات**.
4. بالجزء الأيسر من النافذة، في قسم **إدخال لوحة المفاتيح الآمن**، حدد خانة الاختيار **تمكين إدخال لوحة المفاتيح الآمن**، وانقر فوق زر **الإعدادات**.

   يتم فتح نافذة **إدخال لوحة المفاتيح الآمن**.
5. في النافذة التي يتم فتحها، حدد نطاق الحماية لإدخال البيانات من لوحة مفاتيح الكمبيوتر:

- من علامة التبويب **الفئات**، حدد خانات الاختيار لفئات مواقع الويب التي ينبغي حماية البيانات المدخلة عليها من لوحة المفاتيح.
- إذا كنت تريد حماية إدخال البيانات من لوحة المفاتيح على مواقع الويب التي يتم فتحها في وضع التشغيل الآمن لمواقع الويب في الخدمات النقدية الآمنة، من علامة التبويب **الفئات**، حدد خانة الاختيار **تمكين إدخال لوحة المفاتيح الآمن للخدمات النقدية الآمنة**.
- إذا كنت تريد حماية إدخال البيانات من لوحة المفاتيح في حقول كلمات المرور على كل مواقع الويب، من علامة التبويب **الفئات**، حدد خانة الاختيار **حماية حقول كلمات المرور على كل مواقع الويب**.
- إذا كنت تريد تمكين حماية إدخال البيانات من لوحة المفاتيح على موقع ويب معين:

a. من علامة التبويب **الاستثناءات** في قائمة **تمكين إدخال لوحة المفاتيح الآمن على مواقع الويب**، انقر فوق زر **إضافة**.

   يتم فتح نافذة **موقع الويب المحمي**.

b. في النافذة التي يتم فتحها، أدخل عنوان URL لموقع الويب في حقل **عنوان URL**، وحدد أحد خيارات الحماية لإدخال البيانات على موقع الويب هذا (**تمكين الحماية على صفحة الويب المحددة فقط** أو **تمكين الحماية على موقع الويب بأكمله**).

6. انقر فوق زر **تطبيق** في النافذة **الإعدادات**.

الحماية بكلمة مرور

يقوم Kaspersky PURE بتخزين بياناتك الشخصية وحمايتها (مثل كلمات المرور، وأسماء المستخدم، وتفاصيل الاتصال، والبيانات المالية). يقوم Kaspersky PURE بربط كلمات المرور والحسابات مع التطبيقات أو مواقع الويب المناظرة. يتم احتواء البيانات الشخصية في الحاوية بصيغة مشفرة. تتم حماية الوصول إلى المخزن بكلمة المرور الرئيسية. عند إلغاء تأمين المخزن، يمكنك الوصول إلى كلمات المرور والبيانات بمنتهى السهولة. يقدم Kaspersky PURE طريقة بسيطة ومريحة لإدخال كلمة المرور واسم المستخدم وغيرها من بيانات الهوية عند تسجيل الدخول إلى مواقع الويب أو التطبيقات وكذا تسجيل الدخول تلقائيًا.

يمكنك الوصول إلى بياناتك الشخصية من أي جهاز متصل بالإنترنت ومُثبَّت عليه التطبيق. في حالة اتصال الجهاز بالإنترنت، يمكنك حفظ كلمات المرور والبيانات على الجهاز. بمجرد اتصال الجهاز بالإنترنت، يطالبك Kaspersky PURE بمزامنة كلمات المرور والبيانات مع مخزن كلمات المرور الموجود على الخوادم البعيدة.

يمكنك أيضًا استخدام وظائف Kaspersky PURE من أجل القيام بما يلي:

- إنشاء كلمات مرور قوية للحسابات باستخدام منشئ كلمات المرور
- مزامنة كلمات المرور وبيانات الهوية الحالية مع كافة الأجهزة الخاصة بك المُثبَّت عليها Kaspersky PURE

في هذا القسم

إضافة بيانات الحساب لتسجيل الدخول التلقائي

يمكنك التطبيق من تسجيل الدخول تلقائيًا إلى مواقع الويب والتطبيقات من خلال إدخال تسجيل الدخول وكلمة المرور. يستخدم التطبيقات الحسابات لتسجيل الدخول التلقائي.

يمكنك إنشاء حسابات من نوعين:

- حسابات ويب لتسجيل الدخول إلى مواقع الويب
- حسابات تطبيقات لتسجيل الدخول إلى التطبيقات، مثل تطبيقات البريد الإلكتروني العميلة

لإضافة حساب إنترنت جديد في النافذة الرئيسية لبرنامج Kaspersky PURE:

1. افتح نافذة التطبيق الرئيسية، وانقر فوق زر **مدير كلمات المرور**.

   يتم فتح نافذة مدير كلمات مرور.

2. انقر فوق زر **كلمات المرور والبيانات**.

   يتم عرض محتويات مخزن كلمات المرور والبيانات.

3. افتح قسم **الإنترنت** في نافذة "مدير كلمات المرور".

   تظهر حقوق إدخال تفاصيل الحساب في الجزء الأيسر من النافذة.

4. أدخل اسم الحساب في حقل **اسم الحساب** في الجزء العلوي من النافذة. انقر فوق زر .

   سيتم حفظ اسم الحساب.

5. في حقل **عنوان URL**، أدخل عنوان موقع الويب حيث يتم استخدام الحساب الجديد لتسجيل الدخول إليه.

6. أدخل اسم تسجيل الدخول الخاص بتسجيل الدخول إلى موقع الويب في حقل **تسجيل الدخول**.

7. في مربع النص **كلمة المرور**، أدخل كلمة المرور للحساب. لإنشاء كلمة المرور تلقائيًا، انقر فوق الارتباط **منشئ كلمات المرور**.

8. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

   يظهر الحساب الجديد في قائمة الحسابات في قسم **الإنترنت**.

لإضافة حساب تطبيق جديد:

1. افتح نافذة التطبيق الرئيسية، وانقر فوق زر **مدير كلمات المرور**.

   يتم فتح نافذة مدير كلمات مرور.

2. انقر فوق زر **كلمات المرور والبيانات**.

   يتم عرض محتويات مخزن كلمات المرور والبيانات.

3. افتح قسم **التطبيقات**. انقر فوق زر **إضافة حساب تطبيق**.

4. أدخل اسم الحساب في حقل **اسم الحساب** في الجزء العلوي من النافذة. انقر فوق زر .

   سيتم حفظ اسم الحساب.

5. في حقل **التطبيق**، اكتب المسار إلى الملف القابل للتنفيذ الخاص بالتطبيق الذي ستقوم بتسجيل الدخول إليه من خلال الحساب.

6. أدخل اسم تسجيل الدخول الخاص بتسجيل الدخول إلى التطبيق في حقل **تسجيل الدخول**.

7. في مربع النص **كلمة المرور**، أدخل كلمة المرور للحساب. لإنشاء كلمة المرور تلقائيًا، انقر فوق الارتباط **منشئ كلمات المرور**.

8. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

   يظهر الحساب الذي تم إنشاؤه في قائمة الحسابات في قسم **التطبيقات**.

استخدام منشئ كلمات المرور

يعتمد أمان البيانات بشكل مباشر على قوة كلمات المرور. قد تتعرض البيانات للخطر في الحالات التالية:

- استخدام نفس كلمة المرور لكل الحسابات
- كلمات المرور ضعيفة للغاية
- استخدام معلومات يسهل تخمينها ككلمة مرور (مثل أسماء أو تواريخ ميلاد أفراد العائلة)

وللحفاظ على أمان البيانات، يمكنك Kaspersky PURE من إنشاء كلمات مرور فريدة وقوية للحسابات باستخدام منشئ كلمات المرور.

تعتبر كلمة المرور قوية إذا كانت تتكون من أربعة أحرف أو أكثر، وتحتوي على حروف خاصة وأرقام وأحرف كبيرة وصغيرة.

لإنشاء كلمة مرور قوية باستخدام منشئ كلمات المرور:

1. افتح نافذة التطبيق الرئيسية، وانقر فوق زر **مدير كلمات المرور**.

   يتم فتح نافذة مدير كلمات مرور.

2. انقر فوق زر **منشئ كلمات المرور**.

   يمكنك أيضًا استخدام منشئ كلمات المرور أثناء تحديد كلمة مرور الحساب. ولتشغيل منشئ كلمات المرور، انقر فوق الارتباط **منشئ كلمات المرور** في منطقة إدارة الحسابات بجانب حقل إدخال كلمة المرور.

3. في نافذة **منشئ كلمات المرور** التي تفتح، حدد عدد أحرف كلمة المرور في الحقل**طول كلمة المرور**.

يتراوح طول كلمة المرور بين 4 أحرف و99 حرفًا. تعتبر كلمات المرور الطويلة أكثر قوة.

4. إذا دعت الحاجة، قم بتكوين إعدادات إضافية لمنشئ كلمات المرور من خلال تحديد أو إلغاء تحديد خانات الاختيار بجانب الإعدادات ذات الصلة في القسم **إعدادات متقدمة**.

5. انقر فوق زر **إنشاء**.

يعرض الحقل **كلمة المرور** كلمة المرور التي تم إنشاؤها.

إضافة زوج جديد من بيانات تسجيل الدخول وكلمة المرور

يحتاج المستخدمون أحيانًا إلى استخدام مجموعات مختلفة عديدة من بيانات الاعتماد لتسجيل الدخول لنفس موقع الويب أو التطبيق. ويأتي من بين الأمثلة على ذلك استخدام عدة صناديق بريد على خادم البريد نفسه أو وصول مستخدمين مختلفين إلى حسابات الشبكات الاجتماعية الخاصة بهم من الكمبيوتر نفسه. في هذه الحالة، يوفر Kaspersky PURE إمكانية إنشاء حساب واحد مرتبط بموقع الويب أو التطبيق المعني وتحديد مجموعات عديدة من بيانات الاعتماد لهذا الحساب.

وعند تحميل التطبيق أو موقع الويب المعني، يطلب Kaspersky PURE من المستخدم تحديد بيانات الاعتماد المناسبة لملء حقول تسجيل الدخول.

يكتشف Kaspersky PURE تلقائيًا بيانات تسجيل الدخول الجديدة عند استخدامها لأول مرة، ويطلب من المستخدم إضافتها إلى الحساب الخاص بهذا التطبيق أو موقع الويب. يمكنك إضافة بيانات اعتماد جديدة لأحد الحسابات يدويًا وتحريرها لاحقًا. يمكنك أيضًا اسم نفس بيانات الاعتماد لحسابات مختلفة.

لإضافة زوج جديد من بيانات تسجيل الدخول وكلمة المرور لأحد الحسابات:

1. افتح نافذة التطبيق الرئيسية، وانقر فوق زر **مدير كلمات المرور**.

يتم فتح نافذة مدير كلمات مرور.

2. انقر فوق زر **كلمات المرور والبيانات**.

يتم عرض محتويات مخزن كلمات المرور والبيانات.

3. افتح قسم **الإنترنت** أو **التطبيقات** حسب نوع الحساب الذي تريد إضافة بيانات الاعتماد له.

4. اختر الحساب المعني من القائمة، وانقر فوق زر  .

5. حدد الأمر **إضافة بيانات تسجيل دخول** من القائمة السياقية.

6. أدخل تسجيل الدخول في الحقل **تسجيل الدخول** وكلمة المرور في الحقل **كلمة المرور**.

لإضافة تسجيل دخول وكلمة مرور مستخدمة بالفعل لحسابات أخرى، انقر فوق زر في حقل **تسجيل الدخول**. في حقل **اختيار بيانات الاعتماد المطلوب ربطها** الذي يتم فتحه، حدد الحساب الذي يتضمن بيانات تسجيل الدخول المطلوبة، وانقر فوق زر **ربط**.

7. إذا كنت تريد أن يقوم مدير كلمات المرور تلقائيًا بإدراج بيانات الاعتماد التي قمت بإنشائها على موقع ويب أو أحد التطبيقات، حدد خانة الاختيار **تسجيل الدخول التلقائي** في الجزء السفلي من منطقة إدارة الحسابات.

إذا كانت لا يريد أن يقوم مدير كلمات المرور بإدخال بيانات الاعتماد تلقائيًا في حقول تسجيل الدخول، فلا تحدد خانة الاختيار **تسجيل الدخول تلقائيًا**. في هذه الحالة، يمكنك استخدام تسجيل الدخول التلقائي من خلال تحديد بيانات الاعتماد التي قمت بإنشائها في قائمة السياق للتطبيق أو زر بدء التشغيل السريع.

8. في الجزء السفلي من النافذة، انقر فوق زر **إضافة**.

يظهر عدد بيانات تسجيل الدخول المضافة إلى أحد الحسابات في قائمة الحسابات.

تشفير البيانات

لحماية المعلومات السرية من الوصول غير المصرح به، فإنه من المستحسن أن تقوم بتخزينها في صورة مشفرة في حاوية خاصة.

بشكل افتراضي، تتوفر حاوية فردية سابقة الإعداد تستخدم إعدادات قياسية بعد تثبيت Kaspersky PURE. يتطلب استخدام هذه الحاوية تعيين كلمة مرور. كما يمكن إنشاء الحاويات باستخدام إعدادات مخصصة.

لحماية البيانات، ضعها في الحاوية وقم بتشفيرها. يجب إدخال كلمة المرور للوصول إلى البيانات الموجودة في الحاوية.

لإنشاء حاوية مشفرة:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **تشفير البيانات**.
2. في النافذة التي يتم فتحها، انقر فوق زر **إنشاء حاوية** (راجع الشكل أدناه).

الشكل 9. النافذة تشفير البيانات

3. في النافذة **إنشاء حاوية مشفرة** التي ستفتح، قم بتكوين إعدادات الحاوية الجديدة..

4. انقر فوق **موافق**.

لكتابة بيانات إلى الحاوية:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **تشفير البيانات**.
2. في النافذة التي يتم فتحها، حدد الحاوية من القائمة، وانقر فوق زر **فتح الحاوية**.

   يتم فتح الحاوية في نافذة مستعرض Microsoft Windows.
3. ضع بها البيانات التي ترغب في تشفيرها.
4. في النافذة **تشفير البيانات**، انقر الزر **تشفير البيانات**.

للوصول إلى البيانات في الحاوية، الرجاء القيام بالتالي:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **تشفير البيانات**.
2. في النافذة التي يتم فتحها، حدد الحاوية من القائمة، وانقر فوق زر **فك تشفير البيانات**.
3. في النافذة التي يتم فتحها، أدخل كلمة المرور للوصول إلى الحاوية.
4. في النافذة **تشفير البيانات**، انقر فوق زر **فتح الحاوية**.

أداة مسح البيانات غير المُستخدمة

يقوم النظام بتجميع الملفات المؤقتة أو غير المستخدمة مع مرور الوقت. قد تستغل هذه الملفات مساحة كبيرة على القرص الثابت، مما يؤدي إلى إعاقة أداء النظام كما قد تؤدي أيضًا إلى إمكانية التعرض للبرامج الضارة.

يتم إنشاء الملفات المؤقتة عند بدء تشغيل أي تطبيق أو نظام تشغيل. إلا أن بعضًا من هذه الملفات لا يُحذف عند إغلاق التطبيق أو تشغيل النظام. يأتي Kaspersky PURE مزودًا بالمكون منظف البيانات غير المستخدمة.

تستطيع أداة منظف البيانات غير المستخدمة اكتشاف الملفات التالية وإزالتها:

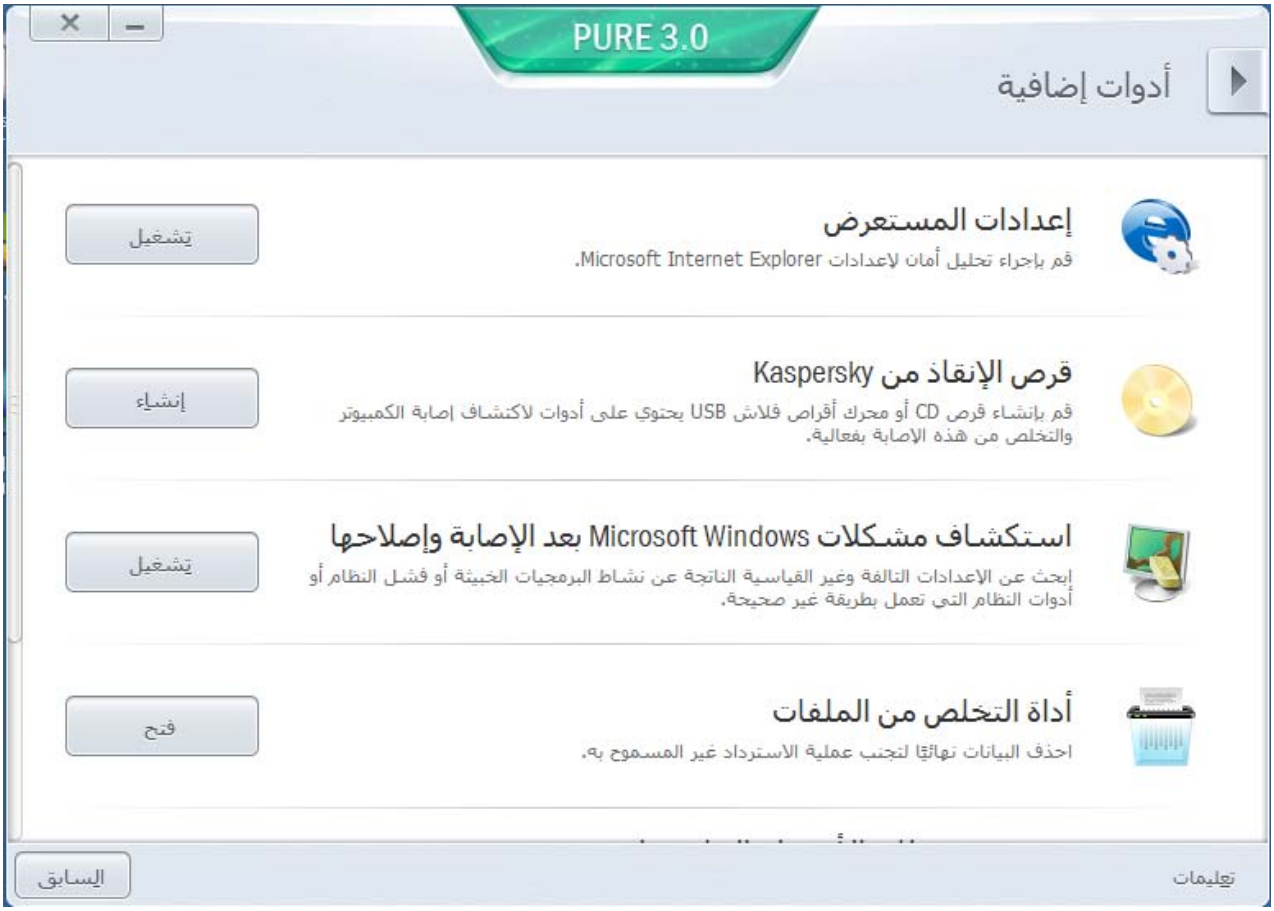
- سجلات أحداث النظام، حيث يتم تسجيل أسماء التطبيقات الفعالة؛
- سجلات أحداث تطبيقات أو أدوات تحديث متنوعة (مثل Windows Updater)؛
- سجلات توصيل النظام؛
- الملفات المؤقتة لمستعرضات الإنترنت (ملفات تعريف الارتباط)؛
- تبقى الملفات المؤقتة بعد تثبيت / إزالة التطبيقات؛
- محتويات سلة المحذوفات؛
- الملفات الموجودة في المجلد Temp التي قد ينمو حجمها ليصل إلى العديد من الجيجا بايت.

وإلى جانب حذف الملفات غير المستخدمة من النظام، يقوم المعالج بحذف الملفات التي قد تحتوي على بيانات شخصية (كلمات المرور وأسماء المستخدم وبيانات من نماذج التسجيل). على الرغم من ذلك، لإتمام حذف مثل هذه البيانات، نوصي باستخدام معالج منظف الخصوصية(انظر صفحة 62)

لبدء تشغيل منظف البيانات غير المستخدمة:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر الزر **أدوات إضافية**.

يتم فتح نافذة **أدوات إضافية** (راجع الشكل الموجود أدناه).



الشكل *10*. نافذة أدوات إضافية

3. في النافذة التي سيتم فتحها، في القسم **منظف البيانات غير المستخدمة**، انقر فوق زر **تشغيل**.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقم بفحص خطوات المعالج بالتفصيل.

الخطوة 1. بدء تشغيل المعالج

توضح الصفحة الأولى من المعالج معلومات حول حذف المعلومات غير المستخدمة

انقر الزر **التالي** لبدء المعالج.

الخطوة 2. البحث عن بيانات غير مستخدمة

يبحث المعالج في الكمبيوتر عن البيانات غير المستخدمة. وقد يستغرق الفحص بعض الوقت. وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 3. تحديد الإجراءات الخاصة بحذف الملفات غير المستخدمة

عند إكمال البحث عن الملفات غير المستخدمة، يُظهر المعالج قائمة بالتطبيقات التي يمكن أن تستخدم هذه الملفات.

لعرض الإجراءات داخل أي مجموعة، انقر الرمز + الموجود على يمين اسم المجموعة.

لجعل المعالج يقوم بتنفيذ إجراء معين، حدد خانة الاختيار الموجودة على يمين وصف الإجراء المعني. وافتراضيًا، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا لم ترغب في تنفيذ إجراء معين، قم بإلغاء تحديد المربع المجاور له.

لا يوصى بإلغاء تحديد خانات الاختيار المحددة بشكل افتراضي. قد يؤدي هذا الأمر إلى تعريض أمان الكمبيوتر الخاص بك للخطر.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر فوق زر **التالي**.

الخطوة 4. أداة مسح البيانات غير المُستخدمة

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. وقد يستغرق حذف المعلومات غير المستخدمة بعض الوقت.

بعد أن ينتهي مسح المعلومات غير المستخدمة، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

أثناء تشغيل النظام، قد تكون بعض الملفات (مثل ملف سجل Microsoft Windows وسجل أحداث Microsoft Office) قيد الاستخدام من قبل النظام. لحذف هذه الملفات، سيقترح المعالج أن تقوم بإعادة تشغيل النظام.

الخطوة 5. اكتمال المعالج

انقر الزر **إنهاء** لإغلاق المعالج.

أداة التخلص من الملفات

يمكنك ضمان الحصول على حماية إضافية للبيانات الشخصية عن طريق حماية البيانات المحذوفة ضد الاستعادة غير المصرح بها بواسطة المهاجمين.

يحتوي Kaspersky PURE على أداة للحذف النهائي للبيانات التي تجعل استعادة البيانات باستخدام أدوات البرامج القياسية أمرًا مستحيلاً.

يجعل Kaspersky PURE من الممكن أن يتم حذف البيانات بدون احتمال استعادتها من وسيط البيانات التالي:

- الأقراص المحلية. يكون الحذف ممكنًا إذا كان للمستخدم الحقوق اللازمة لتسجيل المعلومات وحذفها.
- المحركات القابلة للإزالة أو الأجهزة الأخرى التي يمكن كشفها كمحركات قابلة للإزالة (مثل الأقراص المرنة أو بطاقات الفلاش أو أقراص USB أو الهواتف الخلوية). ويمكن حذف البيانات من بطاقة ذاكرة فلاش إذا كانت الحماية الميكانيكية من إعادة الكتابة معطلة.

يمكنك حذف البيانات التي يمكنك الوصول إليها في حسابك الشخصي. قبل حذف البيانات ، تأكد من أنها غير مستخدمة بواسطة التطبيقات الموجودة قيد التشغيل.

لحذف البيانات دون أي احتمال لاستعادتها:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، انقر الزر **أدوات إضافية**.

يتم فتح نافذة **أداة التخلص من الملفات** (راجع الشكل الموجود أدناه).

الشكل *11*. نافذة أداة التخلص من الملفات

3. في النافذة التي سيتم فتحها، في القسم **أداة التخلص من الملفات**، انقر فوق زر **فتح**.
4. في نافذة **أداة التخلص من الملفات** التي سيتم فتحها، انقر فوق زر **استعراض**، وفي النافذة **تحديد ملف أو مجلد** التي ستفتح حدد ملف أو مجلد ترغب في حذفه بشكل دائم.

قد يتسبب حذف ملفات ومجلدات النظام في أن يعمل نظام التشغيل بشكل غير سليم. إذا حددت ملفات أو مجلدات نظام للحذف، سيطلب التطبيق وجود تأكيد إضافي لطلب الحذف.

5. من القائمة المنسدلة **طريقة حذف البيانات**، حدد الخوارزمية المطلوبة لحذف البيانات.

لحذف البيانات من أجهزة SSD وUSB، إلى جانب محركات الأقراص على الشبكة، يوصى بتطبيق الحذف السريع أو طريقة GOST R 50739-95. قد تضر خوارزميات الحذف الأخرى بأجهزة الشبكة أو الأجهزة القابلة للإزالة.

6. في النافذة التي ستفتح، قم بالتأكيد على استعادة البيانات بالنقر على **موافق**. إذا لم يتم حذف بعض الملفات، حاول مرة أخرى القيام بحذفها بالنقر على الزر **إعادة المحاولة** في النافذة التي ستفتح. ولتحديد كائن آخر لحذفه، انقر الزر **إنهاء**.

منظف الخصوصية

يتم تسجيل إجراءات المستخدم على الكمبيوتر في نظام التشغيل. يتم حفظ المعلومات التالية:

- تفاصيل بحث الاستعلامات التي يقوم المستخدمين ومواقع الويب بإدخالها
- معلومات حول التطبيقات التي تم بدء تشغيلها، والملفات المفتوحة والمحفوظة؛
- إدخالات سجلات أحداث Microsoft Windows؛
- معلومات نشاط المستخدم الأخرى.

معلومات حول إجراءات المستخدم التي تحتوي على معلومات سرية يمكن أن تتوفر للمهاجمين والأشخاص غير المصرح لهم.

يتضمن Kaspersky PURE معالج منظف الخصوصية، الذي يقوم بتنظيف آثار نشاط المستخدم في النظام.

لبدء تشغيل معالج منظف الخصوصية:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، حدد القسم **أدوات إضافية**.
3. في النافذة التي سيتم فتحها، في القسم **منظف الخصوصية**، انقر فوق زر **تشغيل**.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقم بفحص خطوات المعالج بالتفصيل.

الخطوة 1. بدء تشغيل المعالج

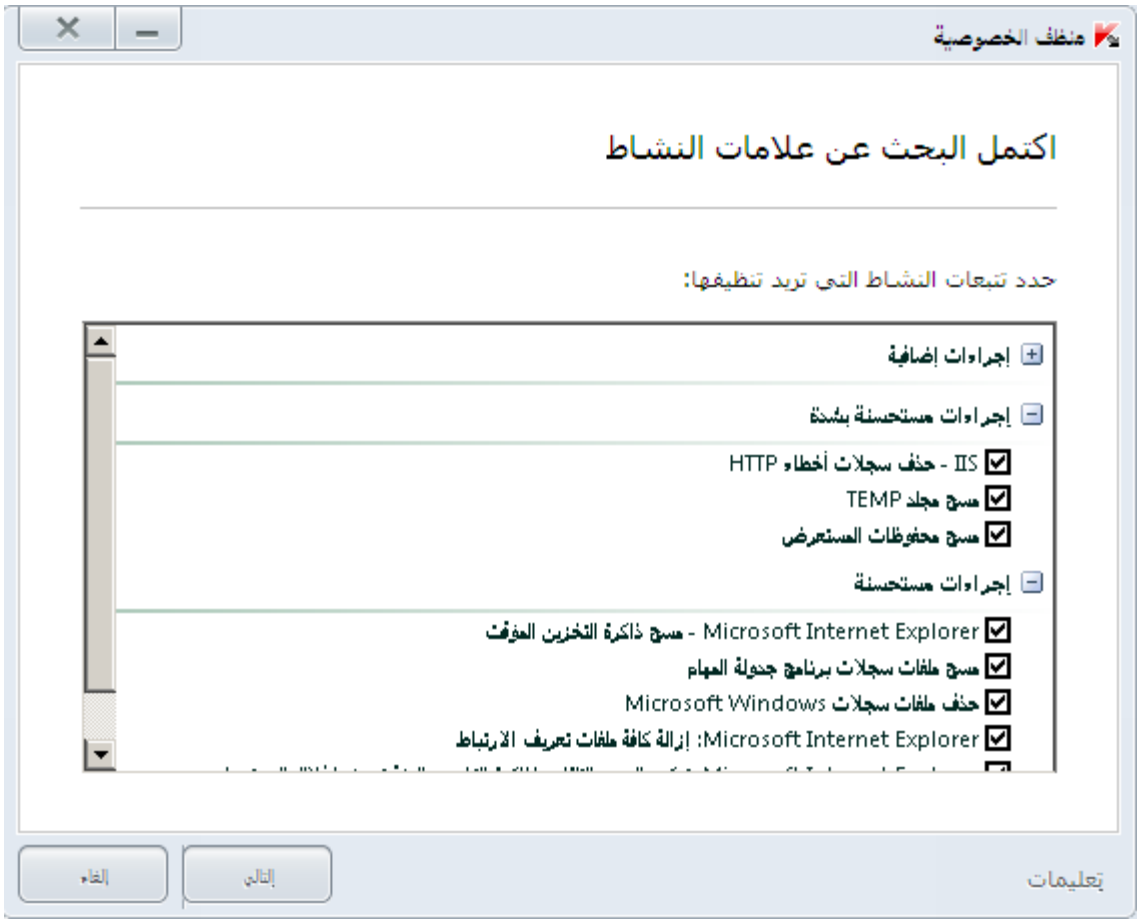
تأكد من أنه تم تحديد الخيار **تنفيذ تشخيص تتبعات نشاط المستخدم** وانقر فوق زر **التالي** لبدء تشغيل المعالج.

الخطوة 2. البحث عن تتبعات النشاط

يقوم هذا المعالج بالبحث عن تتبعات أنشطة البرامج الضارة في جهاز الكمبيوتر. وقد يستغرق الفحص بعض الوقت. وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 3. تحديد إجراءات منظف الخصوصية

عندما يكتمل البحث، يعرض المعالج تتبعات الأنشطة التي عثر عليها والإجراءات المقترحة لإزالتها (راجع الشكل الموجود أدناه).



الشكل *12*. تتبعات النشاط المكتشفة والتوصيات الخاصة بالقضاء عليها

لعرض الإجراءات داخل أي مجموعة، انقر الرمز + الموجود على يمين اسم المجموعة.

لجعل المعالج يقوم بتنفيذ إجراء معين، حدد خانة الاختيار الموجودة على يمين وصف الإجراء المعني. وافتراضيًا، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا لم ترغب في تنفيذ إجراء معين، قم بإلغاء تحديد المربع المجاور له.

لا يوصى بإلغاء تحديد خانات الاختيار المحددة بشكل افتراضي. قد يؤدي هذا الأمر إلى تعريض أمان الكمبيوتر الخاص بك للخطر.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر فوق زر **التالي**.

الخطوة 4. منظف الخصوصية

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. وقد يستغرق التخلص من تتبعات النشاط بعض الوقت. لتنظيف تتبعات أنشطة معينة، قد يكون من المطلوب إعادة تشغيل جهاز الكمبيوتر؛ سيقوم المعالج بإخطارك بها.

وبمجرد أن ينتهي انتظيف تتبعات النشاط، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 5. اكتمال المعالج

إذا كنت ترغب في تنظيف تتبعات نشاط المستخدم تلقائيًا كلما انتهى Kaspersky PURE من عمله، فاستخدم آخر شاشة للمعالج لتحديد خانة الاختيار تنظيف تتبعات النشاط في كل مرة **تنظيف تتبعات النشاط في كل مرة يتم فيها الخروج من Kaspersky PURE 3.0**. وإذا كنت تخطط لإزالة تتبعات النشاط يدويًا باستخدام المعالج، لا تقم بتحديد خانة الاختيار هذه.

انقر الزر **إنهاء** لإغلاق المعالج.

نسخة احتياطية

تعتبر الطريقة الأساسية لتجنب فقد البيانات المهمة هي إنشاء نسخة احتياطية من البيانات على وسيط بيانات يمكن الاعتماد عليه. يقوم Kaspersky PURE بإنشاء نُسخ احتياطية من البيانات المحددة على محرك محدد بشكل تلقائي وفق جدول محدد أو يدويًا.

يمكنك استخدام التحكم في الشبكة المنزلية (راجع القسم"إدارة حماية الشبكة المنزلية عن بُعد" في الصفحة 44) لبدء مهام النسخ الاحتياطي على أجهزة الكمبيوتر المتصلة بالشبكة المنزلية ومراقبة تقدم تلك المهام.

يمكنك استخدام أنواع التخزين الحالية لإنشاء النُسخ الاحتياطية:

- محرك الأقراص المحلي؛
- محرك الأقراص القابل للإزالة (مثل محرك أقراص صلبة خارجي)؛
- محرك أقراص على الشبكة؛
- خادم FTP؛
- التخزين على الإنترنت.

في هذا القسم:

النسخ الاحتياطي للبيانات

لتشغيل النسخ الاحتياطي:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **نسخ احتياطي**.
2. في نافذة **النسخ الاحتياطي** التي ستفتح، انقر فوق زر **إنشاء مهمة نسخ احتياطي**.

سيتم بدء تشغيل معالج إنشاء مهمة النسخ الاحتياطي.

دعنا نقم بفحص خطوات المعالج بالتفصيل:

a. في نافذة تحديد نوع البيانات، قم بأي من العمليات التالية:

- حدد أحد أنواع البيانات سابقة التعيين (الملفات من مجلد "المستندات الخاصة بي" ومجلد "سطح المكتب"، ومقاطع الفيديو، والصور، وملفات الموسيقى) لإجراء التكوين السريع.

- اختر الخيار **ملفات مخصصة** للتحديد اليدوي للملفات المطلوب نسخها احتياطيًا.

b. في حالة تحديد الخيار **ملفات مخصصة** في الخطوة السابقة، حدد الملفات أو فئات الملفات المطلوب نسخها احتياطيًا في نافذة تحديد الملفات.

عند نسخ البيانات في مخزن الإنترنت بشكل احتياطي، لا يقوم Kaspersky PURE بإنشاء نُسخ احتياطية من البيانات التي تخضع أنواعها للقيود التي تفرضها قواعد استخدام Dropbox (انظر القسم "تخزين البيانات على الإنترنت واستخدامها" في الصفحة 66).

c. في نافذة تحديد المخزن، قم بأي من العمليات التالية:

- حدد أحد المخازن سابقة التعيين التي سيتم فيها إنشاء النُسخ الاحتياطية.

بشكل افتراضي، يتيح لك Kaspersky PURE إنشاء نُسخ احتياطية على محركات الأقراص المحلية والقابلة للإزالة، وكذلك في وظيفة التخزين على الإنترنت.

قبل استخدام التخزين على الإنترنت لنسخ البيانات احتياطيًا، يجب عليك تفعيل التخزين على الإنترنت ((راجع القسم "تخزين البيانات على الإنترنت واستخدامها" في الصفحة 66).

- حدد مخزن إنترنت موجودًا.
- انقر فوق زر **إضافة** لإنشاء مخزن إنترنت جديد.

لضمان أمان البيانات، نوصي بإنشاء مخزن الإنترنت أو مخازن النسخ الاحتياطي على محركات أقراص قابلة للإزالة.

d. في نافذة الجدول، قم بتكوين إعدادات بدء تشغيل المهمة.

إذا كنت ترغب في نسخ البيانات احتياطيًا لمرة واحدة فقط، فلا تقم بتحديد خانة الاختيار **التشغيل تلقائيًا حسب الجدول**.

e. في نافذة **الملخص**، أدخل اسم المهمة الجديدة، وحدد خانة الاختيار **تشغيل المهمة عند اكتمال المعالج**، ثم انقر فوق زر **إنهاء**.

استعادة البيانات من النسخ الاحتياطي

لاستعادة البيانات من النسخ الاحتياطي:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **نسخ احتياطي**.
2. حدد القسم **استعادة**.
3. حدد المخزن الذي توجد به النسخ الاحتياطية المطلوبة وانقر الزر **استعادة البيانات**.

سيتم فتح النافذة **استعادة البيانات من التخزين**.

4. في النافذة التي ستفتح، قم بتنفيذ الإجراءات المطلوبة.

a. في القائمة المنسدلة **مهمة النسخ الاحتياطي**، حدد المهمة التي قامت بإنشاء النُسخ الاحتياطية ذات الصلة.

b. في القائمة المنسدلة **التاريخ**، حدد تاريخ ووقت إنشاء النُسخ الاحتياطية ذات الصلة.

c. في القائمة المنسدلة **الفئة**، حدد نوع الملفات المطلوب استعادتها.

5. في قائمة الملفات بالجزء السفلي من النافذة، حدد الملفات المطلوب استعادتها. للقيام بذلك، حدد خانات الاختيار المجاورة للملفات ذات الصلة في القائمة.

لا يتيح Kaspersky PURE استعادة البيانات من التخزين على الإنترنت إذا تم حذف هذه البيانات عبر واجهة Dropbox.

6. انقر فوق زر **استعادة البيانات**.

سيتم فتح النافذة **استعادة**.

7. في النافذة **استعادة**، حدد مكان حفظ الملفات التي تمت استعادتها (المجلد الأصلي أو مجلد مختلف).

8. انقر فوق زر **استعادة البيانات المحددة**.

ستتم استعادة الملفات المحددة للاسترداد وحفظها في المجلد المحدد.

عند اكتشاف إصدار مختلف من أي ملف محدد للاستعادة، يطلب التطبيق من المستخدم استبدال الملف الموجود بالنسخة الاحتياطية أو حفظ كلا الملفين.

استخدام التخزين على الإنترنت

يتيح لك التخزين على الإنترنت حفظ نُسخ احتياطية من بياناتك على خادم بعيد عبر خدمة Dropbox.

لاستخدام التخزين على الإنترنت، قم بإنشاء حساب على موقع الويب الخاص بموفر خدمة النسخ الاحتياطي، وهو Dropbox.

يمكنك استخدام حساب Dropbox واحد لإجراء النسخ الاحتياطي للبيانات من أجهزة مختلفة مُثبت عليها برنامج Kaspersky PURE إلى مخزن إنترنت واحد.

يتيح لك حساب Dropbox القياسي استخدام ما يصل إلى 2 جيجابايت كمساحة خالية على محرك أقراص بعيد واحد. إذا لزم الأمر، فيمكنك زيادة حجم مخزن الإنترنت وفقًا لشروط موفر خدمات النسخ الاحتياطي. راجع موقع Dropbox على الويب لمزيد من التفاصيل حول بنود استخدام خدمة الويب.

قبل استخدام وظيفة التخزين على الإنترنت لنسخ بياناتك احتياطيًا، يجب عليك تنشيطها.

لتنشيط التخزين على الإنترنت:

1. قم بفتح نافذة التطبيق الرئيسية وانقر الزر **نسخ احتياطي**.
2. في نافذة **النسخ الاحتياطي** التي ستفتح، انقر فوق زر **إنشاء مهمة نسخ احتياطي**.

سيتم بدء تشغيل معالج إنشاء مهمة النسخ الاحتياطي.

3. في نافذة تحديد نوع البيانات، حدد فئة البيانات أو حدد يدويًا الملفات التي تريد نسخها احتياطيًا.
4. في نافذة تحديد التخزين، حدد التخزين على الإنترنت، وانقر فوق زر **تنشيط الآن**.

يتم فتح مربع حوار لتسجيل الدخول إلى حساب Dropbox.

5. في النافذة التي يتم فتحها، قم بإحدى العمليات التالية:
   a. أكمل التسجيل إذا لم تكن مستخدم Dropbox مسجلاً.
   b. إذا كنت مستخدم Dropbox مسجلاً، فقم بتسجيل الدخول إلى حسابك على Dropbox.

لإنهاء عملية تنشيط وظيفة التخزين على الإنترنت، تأكد من السماح باستخدام برنامج Kaspersky PURE لحسابك على Dropbox لنسخ البيانات احتياطيًا واستعادتها. يضع Kaspersky PURE نُسخًا احتياطية من البيانات المحفوظة في مجلد منفصل يتم إنشاؤه في مجلد تخزين Dropbox للتطبيقات.

بعد اكتمال عملية تنشيط وظيفة التخزين على الإنترنت، يتم فتح نافذة تحديد المخزن. وهي تتضمن مجموعة من مخازن الإنترنت لتختار منها. بالنسبة لوظيفة التخزين على الإنترنت التي تم تنشيطها، يعرض التطبيق حجم المساحة المستخدمة وحجم المساحة المتاحة لتخزين البيانات.

الوصول المحمي بكلمة المرور إلى إعدادات KASPERSKY PURE

يمكن مشاركة كمبيوتر واحد بواسطة مستخدمين متعددين يمتلكون مستويات مختلفة من الخبرة والمعرفة بالكمبيوتر. قد يؤدي الوصول غير المقيد لعدد من المستخدمين المختلفين إلى Kaspersky PURE والإعدادات الخاصة به إلى تعريض مستوى أمان الكمبيوتر للخطر.

ولتقييد الوصول إلى التطبيق، يمكنك تعيين كلمة مرور المسؤول وتحديد الإجراءات التي ينبغي أن تطلب إدخال كلمة المرور هذه:

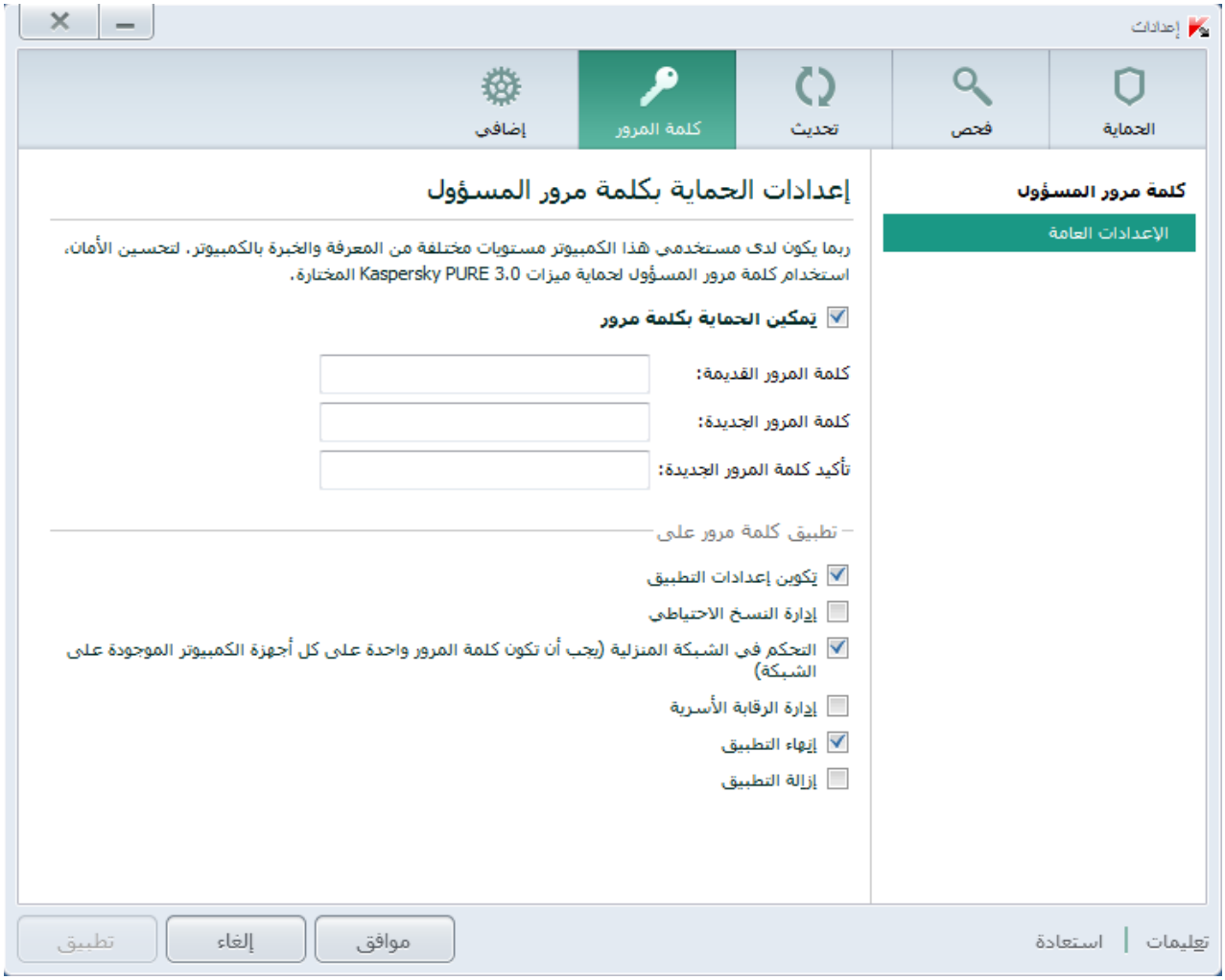
- تكوين إعدادات التطبيق؛
- إدارة النسخ الاحتياطي؛
- التحكم في الشبكة المنزلية (يجب أن تكون كلمة المرور موحدة لكل أجهزة الكمبيوتر الموجودة على الشبكة)؛
- إدارة الرقابة الأسرية؛
- الخروج من التطبيق؛
- إزالة التطبيق.

لحماية الوصول إلى Kaspersky PURE بكلمة مرور:

1. افتح نافذة التطبيق الرئيسية.
2. في الركن الأيسر العلوي من النافذة، انقر فوق الارتباط **الإعدادات**.

سيتم فتح نافذة إعدادات التطبيق.

3. حدد علامة التبويب **كلمة المرور** الموجودة في الجزء العلوي من نافذة الإعدادات (راجع الشكل الموجود أدناه).



الشكل *13*. نافذة الإعدادات، **قسم** كلمة المرور

4. في الجزء الأيسر من النافذة، حدد خانة الاختيار **تمكين الحماية بكلمة المرور**، وأكمل الحقلين **كلمة المرور الجديدة** و**تأكيد كلمة المرور**.

5. لتغيير كلمة مرور تم إنشاؤها من قبل، اكتبها في الحقل **كلمة المرور القديمة**.

6. ضمن مجموعة الإعدادات **تطبيق كلمة المرور على**، حدد عمليات التطبيقات التي ترغب في أن يكون الوصول إليها محميًا بكلمة مرور.

7. انقر فوق زر **تطبيق** لحفظ التغييرات.

لا يمكن استعادة كلمة مرور منسية. إذا نسيت كلمة المرور، فاتصل بالدعم الفني لاستعادة الوصول إلى إعدادات Kaspersky PURE.

استخدام الرقابة الأسرية

تتيح *الرقابة الأسرية* مراقبة الإجراءات التي يتخذها المستخدمون على الكمبيوتر وعلى الإنترنت. يمكنك استخدام الرقابة الأسرية لتقييد الوصول إلى موارد الإنترنت والتطبيقات، إلى جانب إمكانية عرض تقارير حول أنشطة المستخدمين.

وفي الوقت الحالي، يتزايد عدد الأطفال والمراهقين الذين يمكنهم الوصول إلى أجهزة كمبيوتر وموارد الويب. يمثل استخدام أجهزة الكمبيوتر والإنترنت مجموعة كبيرة من المخاطر على الأطفال:

- إهدار الوقت و / أو النقود عند زيارة غرف الدردشة، وموارد الألعاب، والمتاجر على الإنترنت، والمزادات؛
- الوصول إلى مواقع ويب تستهدف البالغين، مثل تلك التي تعرض محتوى يدور حول الإباحية، والتطرف، والأسلحة، وسوء استخدام العقاقير، والعنف الصريح؛
- تنزيل ملفات مصابة ببرمجيات خبيثة؛
- الإضرار بالصحة نتيجة الاستخدام الزائد للكمبيوتر؛
- الاتصال بأشخاص غير مألوفين من الذين يتظاهرون بالصداقة للحصول على معلومات شخصية من المستخدمين الصغار، مثل الاسم الحقيقي، والعنوان الفعلي، والوقت الذي لا يكون فيه أحد موجودًا في المنزل.

يمكنك مكون الرقابة الأسرية من تقليل المخاطر التي يشكلها الكمبيوتر والإنترنت. للقيام بذلك، يتم استخدام وظائف الوحدة النمطية التالية:

- تحديد وقت استخدام الكمبيوتر والإنترنت؛
- إنشاء قوائم بالتطبيقات المسموح بها والممنوعة، بالإضافة إلى التحديد المؤقت لعدد مرات تشغيل التطبيقات المسموح بها؛
- إنشاء قوائم بمواقع الويب المسموح بها والممنوعة، مع تحديد فئات مواقع الويب التي يوصى بعدم عرض محتواها؛
- تمكين وضع البحث الآمن خلال محركات البحث (عدم عرض ارتباطات مواقع الويب التي بها محتوى مريب ضمن نتائج البحث)؛
- تقييد عمليات تحميل الملفات من الإنترنت.
- إنشاء قائمة بجهات الاتصال المسموح أو الممنوع الاتصال بها عبر عملاء المراسلات الفورية والشبكات الاجتماعية.
- عرض سجلات الرسائل من عملاء المراسلات الفورية والشبكات الاجتماعية.
- منع إرسال بيانات شخصية معينة؛
- البحث عن كلمات رئيسية معينة في سجلات الرسائل.

يمكن تمكين كل هذه القيود بشكل منفصل عن إحداها الأخرى، مما يتيح لك تكوين مكون الرقابة الأسرية بشكل مرن لمختلف المستخدمين. وبالنسبة لكل حساب، يمكنك عرض تقارير الأحداث في الفئات التي تتم مراقبتها والتي قام المكون بتسجيلها أثناء مدة محددة.

في هذا القسم:

تكوين الرقابة الأسرية

إذا لم تكن قد قمت بإجراء حماية الوصول إلى إعدادات Kaspersky PURE باستخدام كلمة مرور (راجع الصفحة 67)، سيقوم مكون الرقابة الأسرية من Kaspersky PURE باقتراح قيامك بتعيين كلمة مرور لمنح التغييرات غير المصرح بها لإعدادات التحكم

عند تشغيله للمرة الأولى. وبعد ذلك، يمكنك تكوين قيود على استخدام الكمبيوتر والإنترنت بواسطة الحسابات الموجودة على الكمبيوتر.

لتكوين الرقابة الأسرية للحساب:

1. افتح نافذة التطبيق الرئيسية وانقر الزر **الرقابة الأسرية**.

سيتم فتح النافذة **مستخدمو الكمبيوتر**، مع سرد جميع حسابات المستخدمين التي تم إنشاؤها على الكمبيوتر.

2. انقر فوق زر **تحديد مستوى المراقبة** للحساب ذي الصلة.
3. في النافذة **الرقابة الأسرية** التي يتم فتحها، قم بتنفيذ أي مما يلي:

- حدد أحد مستويات المراقبة سابقة الإعداد (**تجميع البيانات** أو **ملف تعريف الطفل** أو **ملف تعريف المراهق**)
- تعيين القيود يدويًا:

a. حدد العنصر **قيود مخصصة**.

b. انقر فوق زر **إعدادات**.

ستفتح النافذة **الرقابة الأسرية**.

c. في النافذة التي يتم فتحها، من علامة تبويب **الإعدادات**، حدد نوع القيد في الجزء الأيمن من النافذة، وحدد إعدادات التحكم في الجزء الأيسر من النافذة.

d. انقر فوق زر **موافق** لحفظ إعدادات التحكم المكونة.

4. انقر فوق زر **موافق** في النافذة **الرقابة الأسرية**.

عرض تقرير حول نشاط المستخدم

يمكنك الوصول إلى تقارير حول نشاط كل حساب مستخدم موضوع تحت الرقابة الأسرية، وذلك لمراجعة كل فئة من الأحداث الخاضعة للتحكم على حدة.

لعرض تقرير حول نشاط حساب مستخدم خاضع للتحكم:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، حدد القسم **الرقابة الأسرية**.
3. في القسم الذي يحتوي على الحساب بالنافذة التي يتم فتحها، انقر فوق زر  .

ستفتح النافذة **الرقابة الأسرية**.

4. حدد علامة التبويب **التقارير**.
5. استخدم الجزء الأيمن من النافذة التي ستفتح لتحديد فئة العمليات أو المحتوى الذي تتم مراقبته، مثل **استخدام الإنترنت** أو **بيانات خاصة**.

سيتم عرض تقرير بالإجراءات والمحتوى التي تتم مراقبته في الجزء الأيسر من النافذة.

إيقاف حماية الكمبيوتر واستعادتها

يعني الإيقاف المؤقت للحماية التعطيل المؤقت لجميع مكونات الحماية لبعض الوقت.

لإيقاف حماية الكمبيوتر مؤقتًا:

1. من قائمة سياق رمز التطبيق الموجودة في منطقة إخطارات شريط المهام، حدد العنصر **إيقاف الحماية مؤقتًا**.

   يتم فتح النافذة **إيقاف الحماية مؤقتًا** (راجع الشكل الموجود أدناه).

الشكل *14*. النافذة إيقاف الحماية مؤقتًا

2. في النافذة **إيقاف الحماية مؤقتًا** التي ستفتح، حدد الفاصل الزمني الذي ينبغي استئناف الحماية بعد انقضائه:

- **إيقاف مؤقت لمدة محددة** – سيتم تمكين الحماية بعد انتهاء الفاصل الزمني المحدد من القائمة المنسدلة أدناه.
- **إيقاف مؤقت حتى إعادة التشغيل** – سيتم تمكين الحماية بعد إعادة تشغيل التطبيق أو نظام التشغيل (بشرط تمكين بدء التشغيل التلقائي للتطبيق).
- **الإيقاف المؤقت** – سيتم استئناف الحماية بعد أن تقرر أنت استئنافها.

لاستئناف حماية الكمبيوتر،

حدد العنصر **متابعة الحماية** في قائمة سياق التطبيق الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام.

عرض تقرير حماية الكمبيوتر

يحتفظ Kaspersky PURE بتقارير تشغيل كل مكون من مكونات الحماية. يوفر التقرير معلومات إحصائية حول تشغيل التطبيق (مثل عدد الكائنات الخبيثة المكتشفة والتي تم إبطالها خلال فترة معينة، وعدد تحديثات التطبيق خلال الفترة نفسها، وعدد رسائل البريد الإلكتروني غير المرغوب فيه المكتشفة، وغير ذلك المزيد).

لعرض تقرير حول حماية الكمبيوتر:

1. افتح نافذة التطبيق الرئيسية، وانقر الزر **حماية جهاز الكمبيوتر**.

تفتح النافذة **حماية جهاز الكمبيوتر**.

2. انقر فوق ارتباط **التقارير** في الجزء العلوي من النافذة لفتح نافذة تقارير حماية الكمبيوتر.

تظهر تقارير حماية الكمبيوتر كرسومات بيانية في النافذة **التقارير**.

3. إذا رغبت في عرض تقرير مفصل حول نشاط التطبيق (على سبيل المثال، تقرير حول نشاط كل مكون)، انقر فوق زر **تقرير تفصيلي** في الجزء السفلي من نافذة **التقرير**.

تفتح النافذة **تقرير تفصيلي** وتعرض البيانات في جدول. ولسهولة عرض التقارير، يمكنك تحديد العديد من خيارات الفرز.

استعادة إعدادات التطبيق الافتراضية

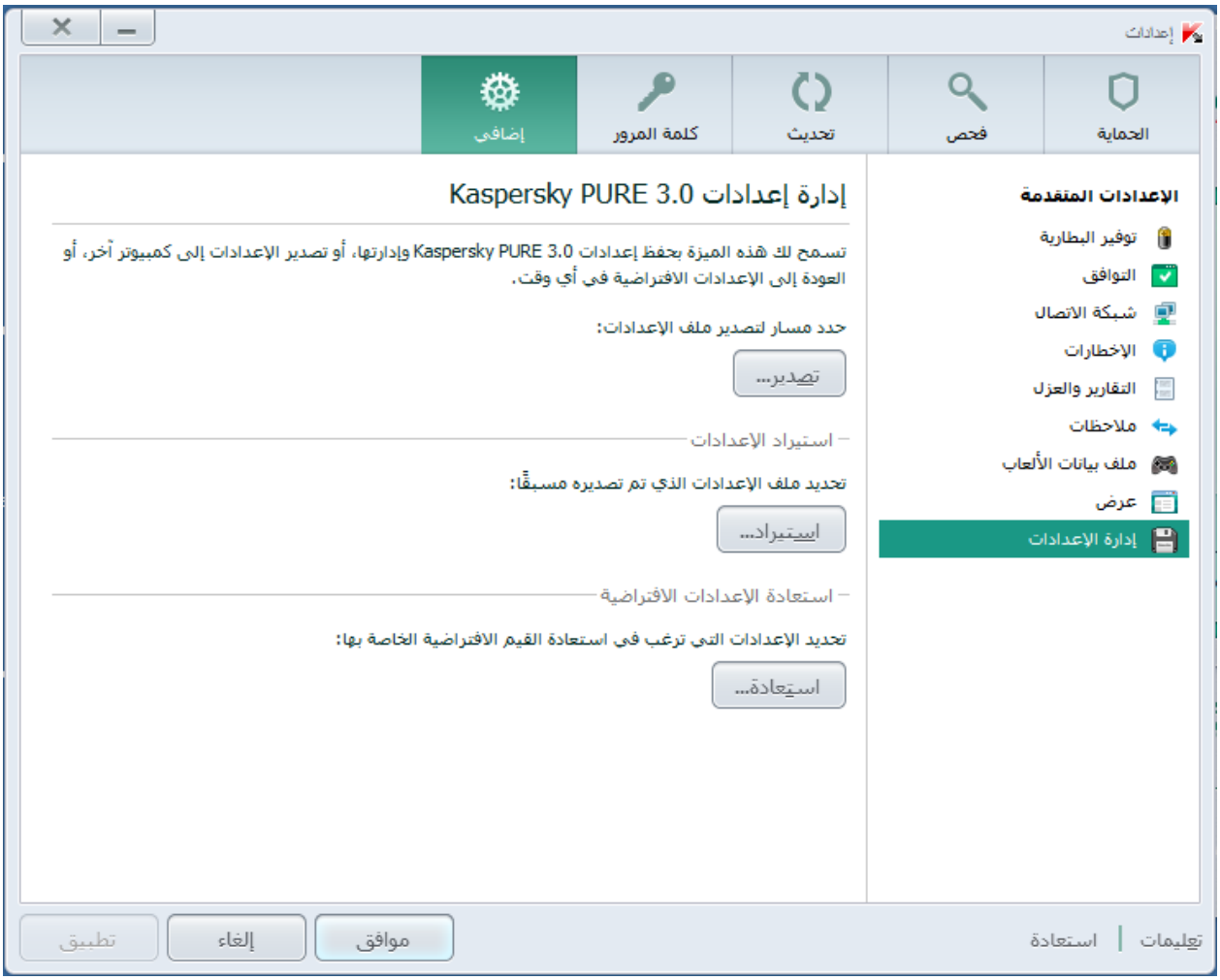
يمكنك استعادة إعدادات التطبيق الافتراضية التي توصي بها Kaspersky Lab لبرنامج Kaspersky PURE في أي وقت تريد. ويمكن استعادة الإعدادات باستخدام معالج تكوين التطبيق.

يقوم معالج تكوين التطبيق بتعيين مستوى الأمان *المستحسن* لجميع مكونات الحماية. عند استعادة مستوى الأمان الموصى به، يمكنك حفظ القيم المحددة من قبل لبعض إعدادات مكونات التطبيق.

لاستعادة الإعدادات المستحسنة للتطبيق:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في نافذة **الإعدادات** التي يتم فتحها، قم بتشغيل معالج تكوين التطبيق بأي من الطرق التالية:
   - انقر فوق الارتباط **استعادة** في الركن السفلي الأيمن من النافذة؛

- في الجزء العلوي من النافذة، حدد قسم **الإعدادات المتقدمة**، وحدد القسم الفرعي **إدارة الإعدادات**، وانقر فوق زر **استعادة** في قسم **استعادة الإعدادات الافتراضية** (انظر الشكل أدناه).



الشكل 15. نافذة الإعدادات، **القسم الفرعي** إدارة الإعدادات

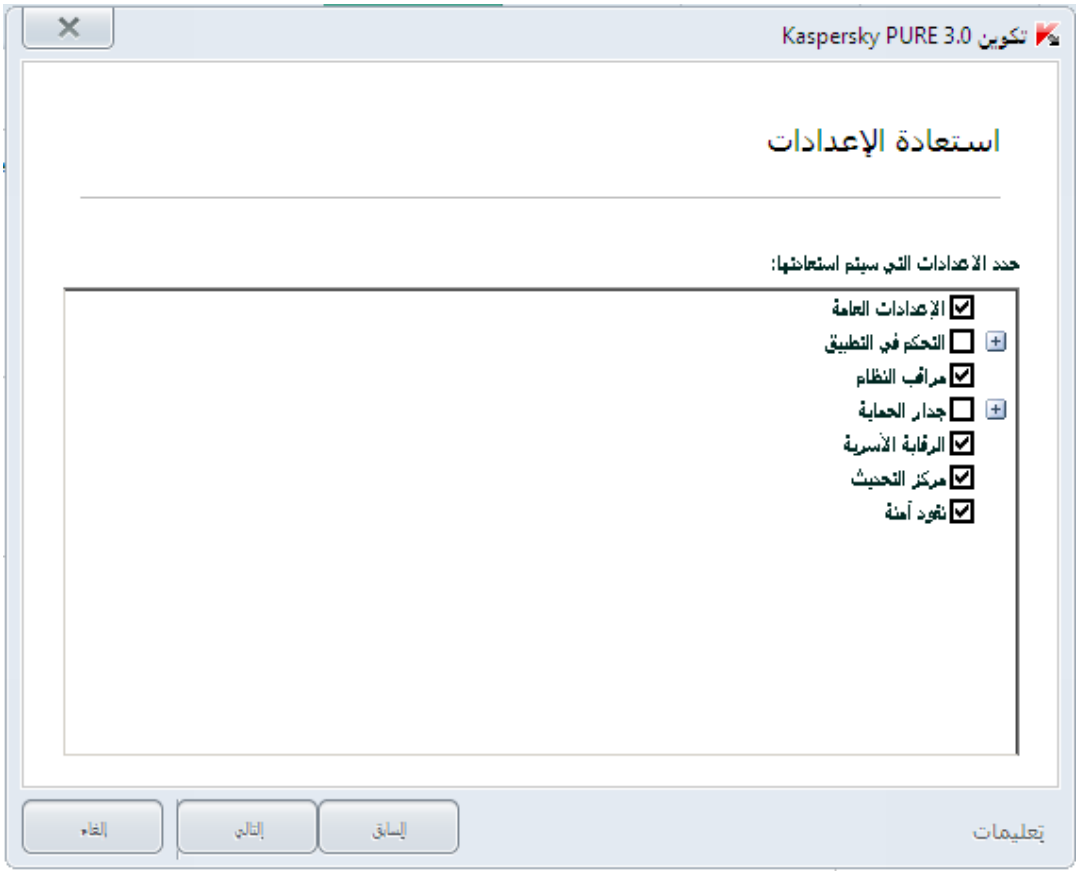
دعنا نقم بفحص خطوات المعالج بالتفصيل.

الخطوة 1. بدء تشغيل المعالج

انقر الزر **التالي** لمتابعة التثبيت.

الخطوة 2. استعادة الإعدادات

تعرض نافذة المعالج هذه مكونات حماية Kaspersky PURE التي لها إعدادات مختلفة عن القيمة الافتراضية نظرًا لأنه تم تغييرها بواسطة المستخدم أو تجميعها بواسطة Kaspersky Internet Security خلال التدريب (جدار الحماية أو مكافحة البريد الإلكتروني غير المرغوب فيه). في حالة إنشاء إعدادات خاصة لأي من المكونات، سيتم إظهارها أيضًا في النافذة (راجع الشكل الموجود أدناه).



الشكل 16. النافذة استعادة الإعدادات

من أمثلة الإعدادات الخاصة: القوائم البيضاء والسوداء للعبارات والعناوين المستخدمة بواسطة مكون مكافحة البريد العشوائي وقوائم عناوين URL الموثوق بها وأرقام هاتف ISP الموثوق بها وقواعد الاستثناء التي تم إنشائها لمكونات التطبيق وحزمة جدار الحماية وقواعد تصفية التطبيق.

يتم إنشاء الإعدادات الخاصة عند العمل مع Kaspersky PURE فيما يتعلق بالمهام الفردية ومتطلبات الأمان. توصيك Kaspersky Lab بحفظ إعداداتك الخاصة عند استعادة إعدادات التطبيق الافتراضية.

حدد خانات الاختيار المقابلة للإعدادات التي يجب الاحتفاظ بها وانقر فوق **التالي**.

الخطوة 3. تحليل النظام

عند هذه المرحلة، يتم تجميع المعلومات الخاصة بالتطبيقات المضمنة مع Microsoft Windows. تتم إضافة هذه التطبيقات إلى قائمة التطبيقات الموثوق بها الخالية من القيود الخاصة بالإجراءات التي يتم تنفيذها على النظام.

وبمجرد أن يكتمل التحليل، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 4. إكمال الاستعادة

ولإنهاء عمل المعالج، انقر الزر **إنهاء**.

استيراد إعدادات التطبيق إلى KASPERSKY PURE المثبت على كمبيوتر آخر

بعد تكوين المنتج، يمكنك تطبيق إعداداته على Kaspersky PURE المُثبَّت على كمبيوتر آخر. وبالتالي، سيتم تكوين التطبيق بشكل متماثل على كلا جهازي الكمبيوتر. هذه الميزة مفيدة عندما يكون Kaspersky PURE مثبتًا بجهاز الكمبيوتر بالمنزل أو بالمكتب على سبيل المثال.

يمكن نقل إعدادات Kaspersky PURE إلى كمبيوتر آخر من خلال ثلاث خطوات:

1. تصدير إعدادات التطبيق إلى ملف تكوين.
2. نقل ملف تكوين إلى كمبيوتر آخر (عبر البريد الإلكتروني أو على وسائط قابلة للإزالة مثلاً).
3. تطبيق الإعدادات من ملف تكوين على التطبيق المُثبَّت على كمبيوتر آخر.

لحفظ إعدادات Kaspersky PURE في ملف التكوين:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في الجزء العلوي من نافذة **الإعدادات** بقسم **إضافي**، حدد القسم الفرعي **إدارة الإعدادات**.
4. انقر فوق زر **تصدير** في القسم الفرعي **إدارة الإعدادات**.
5. في النافذة التي يتم فتحها، أدخل اسم ملف التكوين، وحدد الموقع الذي ينبغي حفظه فيه.
6. انقر فوق **موافق**.

لتطبيق الإعدادات من ملف التكوين على التطبيق المُثبَّت على كمبيوتر آخر:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط **الإعدادات** في الجزء العلوي من النافذة.
3. في الجزء العلوي من نافذة **الإعدادات** بقسم **إضافي**، حدد القسم الفرعي **إدارة الإعدادات**.
4. انقر فوق زر **استيراد** في القسم الفرعي **إدارة الإعدادات**.
5. في النافذة التي يتم فتحها، حدد الملف الذي ترغب في استيراد إعدادات Kaspersky PURE منه.
6. انقر فوق **موافق**.

إنشاء قرص الإنقاذ واستخدامه

ويعتبر قرص الإنقاذ عبارة عن نسخة من قرص الإنقاذ من Kaspersky محفوظ على محرك قابل للإزالة (قرص مضغوط أو جهاز USB).

يمكنك استخدام قرص الإنقاذ من Kaspersky لفحص وتنظيف أجهزة الكمبيوتر المصابة التي يتعذر تنظيفها باستخدام الطرق الأخرى (على سبيل المثال، باستخدام تطبيقات مكافحة الفيروسات).

في هذا القسم:

إنشاء قرص الإنقاذ

تتكون عملية إنشاء قرص إنقاذ من إنشاء صورة قرص (ملف ISO) بها الإصدار المُحدَّث من قرص إنقاذ Kaspersky وحفظها على وسائط قابلة للإزالة.

يمكن تحميل صورة القرص الأصلي من خادم Kaspersky Lab أو نسخها من مصدر محلي.

يتم إنشاء قرص الإنقاذ باستخدام معالج إنشاء قرص الإنقاذ من Kaspersky. ويحفظ ملف rescued.iso الذي تم إنشاؤه بواسطة المعالج على القرص الثابت بجهاز الكمبيوتر.

- في Microsoft Windows XP – في المجلد التالي: Documents and Settings\All Users\Application Data\Kaspersky\Lab\AVP13\Data\Rdisk؛
- في أنظمة التشغيل Microsoft Windows Vista، وMicrosoft Windows 7، وMicrosoft Windows 8 – في المجلد التالي: \ProgramData\Kaspersky Lab\AVP13\Data\Rdisk.

لإنشاء قرص إنقاذ:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، حدد القسم **أدوات إضافية**.
3. في النافذة **قرص الإنقاذ من Kaspersky** التي ستفتح، انقر فوق زر **حفظ**.

سيتم فتح النافذة **معالج إنشاء قرص الإنقاذ**.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يتم التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.

دعنا نقم بفحص خطوات المعالج بالتفصيل.

الخطوة 1. بدء تشغيل المعالج. البحث عن صورة قرص موجودة

توضح الصفحة الأولى من المعالج معلومات حول تطبيق قرص الإنقاذ من Kaspersky.

إذا قام المعالج باكتشاف وجود صورة قرص تم إنشاؤها مسبقًا في المجلد لهذا الغرض (راجع أعلاه)، ستظهر خانة الاختيار **استخدام صورة قرص الإنقاذ من Kaspersky الموجودة** على الصفحة الأولى من المعالج. حدد خانة الاختيار لاستخدام الملف المكتشف كصورة ISO الأصلية، ثم انتقل مباشرة إلى خطوة **تحديث صورة القرص** (انظر أدناه). إذا لم تكن ترغب في استخدام صورة القرص الموجودة، قم بمسح خانة الاختيار هذه. سيتابع المعالج إلى الصفحة **تحديد مصدر صورة القرص**.

الخطوة 2. حدد مصدر صورة القرص

إذا كنت قد قمت بتحديد خانة الاختيار **استخدام صورة قرص الإنقاذ من Kaspersky موجودة** في الصفحة الأولى للمعالج، سيتم تخطي هذه الخطوة.

عند هذه الخطوة يجب عليك تحديد مصدر صورة القرص من قائمة الخيارات:

- إذا كان لديك قرص إنقاذ من Kaspersky مسجل بالفعل أو صورة منه (ملف ISO) محفوظة على الكمبيوتر الخاص بك أو على مورد شبكة آخر، فحدد الخيار **نسخ صورة ISO من محرك الأقراص المحلي أو محرك الأقراص على الشبكة**.
- إذا لم يكن لديك صورة قرص إنقاذ مسجلة وترغب في تنزيله من خادم Kaspersky Lab (يصل الحجم التقريبي للملف إلى 175 ميجا بايت)، حدد الخيار **تنزيل صورة ISO من خادم Kaspersky Lab**.

الخطوة 3. نسخ (تحميل) صورة القرص

إذا كنت قد قمت بتحديد خانة الاختيار **استخدام صورة قرص الإنقاذ من Kaspersky موجودة** في الصفحة الأولى للمعالج، سيتم تخطي هذه الخطوة.

إذا قمت بتحديد الخيار **نسخ صورة ISO من محرك الأقراص المحلي أو محرك الأقراص على الشبكة** خلال الخطوة السابقة، فانقر فوق زر **استعراض**. بعد قيامك بتحديد مسار الملف، انقر الزر **التالي**. يتم عرض تقدم نسخ صورة القرص في نافذة المعالج.

إذا قمت بتحديد **تنزيل صورة ISO من خادم Kaspersky Lab** خلال الخطوة السابقة، سيتم عرض حالة تقدم تنزيل صورة القرص على الفور.

عند انتهاء نسخ صورة ISO أو تحميلها، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

الخطوة 4. تحديث ملف صورة ISO

يتكون إجراء التحديث الخاص بملف صورة ISO من العمليات التالية:

- تحديث قواعد بيانات التطبيق
- تحديث ملفات التكوين.

تحدد ملفات التكوين ما إذا كان يمكن بدء تشغيل الكمبيوتر من وسائط قابلة للإزالة (مثل قرص CD / DVD أو محرك أقراص فلاش USB بقرص الإنقاذ من Kaspersky) يتم إنشاؤها بواسطة المعالج.

عند تحديث قواعد بيانات التطبيق، يتم استخدام قواعد البيانات التي تم توزيعها في آخر تحديث لبرنامج Kaspersky PURE. إذا كانت قواعد البيانات قديمة، فيوصى بتشغيل مهمة التحديث وبدء تشغيل معالج إنشاء قرص الإنقاذ من Kaspersky مرة أخرى.

لبدء تحديث ملف صورة القرص، انقر الزر **التالي**. سيتم عرض تقدم التحديث في نافذة المعالج.

الخطوة 5. تسجيل صورة القرص على المحرك

عند هذه الخطوة، يعلن المعالج إنشاء صورة القرص بنجاح ويعرض كتابة صورة القرص إلى المحرك.

حدد المحرك الذي يجب كتابة قرص الإنقاذ من Kaspersky عليه:

- لتسجيل صورة القرص على قرص CD / DVD، حدد **تسجيل على قرص CD / DVD**، وحدد الوسائط التي تريد عليها تسجيل صورة القرص.

- للكتابة إلى جهاز USB، حدد الخيار **تسجيل على محرك أقراص فلاش USB**، وحدد الجهاز الذي تريد كتابة صورة القرص إليه.

لا يوصي المتخصصين في Kaspersky Lab بحفظ صورة القرص على أجهزة لا تهدف بشكل حصري إلى تخزين البيانات، مثل الهواتف الذكية أو الهواتف المحمولة أو أجهزة كمبيوتر الجيب أو مشغلات MP3. فقد لا تعمل هذه الأجهزة بشكل جيد بعد استخدامها لتخزين صورة القرص.

- لحفظ صورة القرص على المحرك الثابت للكمبيوتر الخاص بك أو لجهاز كمبيوتر آخر يمكنك الوصول إليه عبر الشبكة، حدد الخيار **حفظ صورة القرص إلى ملف موجود على محرك محلي أو على الشبكة** وحدد المجلد الذي ترغب في حفظ صورة القرص عليه وحدد اسم ملف ISO.

الخطوة 6. اكتمال المعالج

ولإنهاء عمل المعالج، انقر الزر **إنهاء**. يمكنك استخدام قرص الإنقاذ الذي تم إنشاؤه مؤخرًا في إعادة تشغيل الكمبيوتر (راجع الصفحة 78) إذا كنت لا تستطيع تشغيله وتقوم بتشغيل Kaspersky PURE في الوضع العادي بسبب الأثر الناجم عن الفيروسات أو البرامج الضارة.

تمهيد الكمبيوتر باستخدام قرص الإنقاذ

في حالة تعذر بدء نظام التشغيل نتيجة لهجوم من فيروس، استخدم قرص الإنقاذ.

لتمهيد نظام التشغيل، ينبغي استخدام قرص مضغوط أو قرص DVD أو محرك فلاش USB منسوخ عليه قرص إنقاذ Kaspersky (راجع القسم "إنشاء قرص إنقاذ" في الصفحة 76).

لا يكون تحميل الكمبيوتر من محرك أقراص قابل للإزالة أمرًا ممكنًا في جميع الأحيان. وبوجه خاص، لا تدعم بعض الطرازات القديمة لأجهزة الكمبيوتر هذا الوضع. وقبل إيقاف تشغيل الكمبيوتر للتمهيد مرة أخرىمن وسيط بيانات قابل للإزالة، تأكد من إمكانية تنفيذ هذه العملية.

لتمهيد الكمبيوتر باستخدام قرص الإنقاذ

1. في إعدادات BIOS، قم بتمكين التشغيل من قرص CD / DVD أو جهاز USB (للحصول على معلومات تفصيلية، برجاء الرجوع إلى الوثائق الخاصة باللوحة الأم للكمبيوتر الخاص بك).
2. أدخل قرص CD / DVD في محرك أقراص CD / DVD الخاص بالكمبيوتر المصاب، وقم بتوصيل جهاز فلاش USB منسوخ عليه قرص الإنقاذ من Kaspersky.
3. أعد تشغيل الكمبيوتر.

للحصول على معلومات مفصلة حول استخدام قرص الإنقاذ، الرجاء الرجوع إلى دليل مستخدم قرص الإنقاذ من Kaspersky.

الاتصال بخدمة الدعم الفني

يوفر هذا القسم معلومات حول كيفية الحصول على الدعم الفني ومتطلبات تلقي التعليمات من الدعم الفني.

في هذا القسم

كيفية الحصول على الدعم الفني

إذا لم تجد حلاً للمشكلة التي تواجهك في وثائق التطبيق أو في أحد مصادر المعلومات الخاصة بالتطبيق (راجع القسم "مصادر المعلومات المتعلقة بالتطبيق" (على الصفحة 9))، فإننا نوصيك بالاتصال بخدمة الدعم الفني لـ Kaspersky Lab. وسوف يجيب أخصائيو الدعم الفني على أي من تساؤلاتك حول تثبيت التطبيق واستخدامه.

قبل الاتصال بخدمة الدعم الفني، الرجاء قراءة قواعد الدعم (http://support.kaspersky.com/support/rules).

يمكنك الاتصال بخدمة الدعم الفني بإحدى الطرق التالية:

- عبر الهاتف. تتيح لك هذه الطريقة إمكانية استشارة الأخصائيين من الدعم الفني باللغة الروسية أو الدعم الفني العالمي.
- عن طريق إرسال استعلام من حساب Kaspersky الخاص بك الموجود على موقع خدمة الدعم الفني على الويب. تتيح لك هذه الطريقة إمكانية الاتصال بأخصائيي الدعم الفني من خلال نموذج طلب.

يتوفر الدعم الفني فقط للمستخدمين الذين قاموا بشراء الترخيص التجاري. لن يتم توفير الدعم الفني لمستخدمي الإصدارات التجريبية.

الدعم الفني عبر الهاتف

في حالة حدوث مشكلة ملحة، يمكنك الاتصال بالمتخصصين الذين يتحدثون الروسية أو القسم العالمي لقسم الدعم الفني (http://support.kaspersky.com/support/international) بواسطة الهاتف.

قبل الاتصال بخدمة الدعم الفني، الرجاء قراءة قواعد الدعم (http://support.kaspersky.com/support/details). فإن هذا سيمكن خبراءنا من تقديم المساعدة بشكل أسرع.

الحصول على الدعم الفني من خلال حسابي في KASPERSKY

يعد *حسابي في Kaspersky* عبارة عن منطقتك الشخصية (https://my.kaspersky.com) على موقع الدعم الفني على الويب.

للحصول على حق الوصول إلى حسابي في Kaspersky، يجب تنفيذ إجراءات التسجيل الموجودة على صفحة التسجيل (https://my.kaspersky.com/registration). أدخل عنوان البريد الإلكتروني الخاص بك وكلمة مرور لتسجيل الدخول في حسابي في Kaspersky.

في حسابي في Kaspersky، يمكنك تنفيذ الإجراءات التالية:

- الاتصال بالدعم الفني ومعمل الفيروسات.
- الاتصال بالدعم الفني دون استخدام البريد الإلكتروني.
- تتبع حالة طلباتك في الحال.
- عرض سجل تفصيلي بطلباتك المتعلقة بالدعم الفني.
- استلام نسخة من ملف المفتاح في حالة فقده أو حذفه.

الدعم الفني باستخدام البريد الإلكتروني

يمكنك إرسال طلب عبر الإنترنت إلى الدعم الفني باللغة الإنجليزية، أو الروسية، أو الألمانية، أو الفرنسية، أو الإسبانية.

في حقول نموذج الطلب عبر الإنترنت، حدد البيانات التالية:

- نوع الطلب
- اسم التطبيق ورقم الإصدار
- وصف الطلب
- مُعرِّف العميل وكلمة المرور
- عنوان البريد الإلكتروني

سيقوم أحد المتخصصين في خدمة الدعم الفني بإرسال إجابة إلى طلبك إلى حساب Kaspersky الخاص بك وإلى عنوان البريد الإلكتروني الذي حددته في طلبك المقدم عبر الإنترنت.

طلب عبر الإنترنت إلى معمل الفيروسات

يجب إرسال بعض الطلبات إلى معمل الفيروسات بدلاً من الدعم الفني.

يمكنك إرسال طلبات الأنواع التالية إلى معمل الفيروسات:

- *برمجيات خبيثة غير معروفة* – تشك في أن الملف يحتوي على فيروس، ولكن لا يقوم Kaspersky PURE بتحديده كملف مصاب.

  يقوم المتخصصون في معمل الفيروسات بتحليل الرمز الخبيث المرسل. إذا اكتشفوا فيروسًا مجهولاً من قبل، فإنهم يقومون بإضافة وصف متطابق إلى قاعدة البيانات والذي يصبح متاحًا عند تحديث تطبيقات مكافحة الفيروسات.

- *اكتشاف إيجابي زائف* – يقوم Kaspersky PURE بتصنيف الملف على أنه فيروس، ولكنك متأكد من أن هذا الملف ليس فيروسًا.

- *طلب وصف البرنامج الخبيث* – أنت تريد استقبال وصف لفيروس اكتشفه Kaspersky PURE وفقًا لاسم الفيروس.

يمكنك أيضًا إرسال طلبات إلى معمل مكافحة الفيروسات من الصفحة التي تحتوي على نموذج الطلب (http://support.kaspersky.com/virlab/helpdesk.html) بدون التسجيل في حسابي في Kaspersky. من هذه الصفحة، ليس عليك تحديد رمز تنشيط التطبيق.

إنشاء تقرير لحالة النظام واستخدام برامج AVZ النصية

بعد أن تقوم بإخطار متخصصي خدمة الدعم الفني بالمشكلة التي تواجهها، قد يطلبون منك إنشاء تقرير ينبغي أن يتضمن معلومات حول نظام التشغيل الخاص بك وإرساله إلى خدمة الدعم الفني. قد يطلب منك أيضًا متخصصو خدمة الدعم الفني إنشاء ملف يضم معلومات فنية حول أداء النظام. يساعد هذا الملف على تتبع تنفيذ أوامر التطبيق خطوة بخطوة واكتشاف مرحلة عملية التطبيق عند حدوث الخطأ.

بعد أن يقوم متخصصو خدمة الدعم الفني بتحليل البيانات التي قمت بإرسالها، يمكنهم إنشاء برنامج AVZ نصي وإرساله إليك. يسمح لك تشغيل برامج AVZ النصية بتحليل العمليات النشطة للرمز الخبيث وفحص النظام بحثًا عن الرمز الخبيث وتنظيف/حذف الملفات المصابة وإنشاء تقارير تضم نتائج عمليات فحص النظام.

في هذا القسم:

إنشاء تقرير حالة النظام

لإنشاء تقرير حالة النظام:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق ارتباط **الدعم** في الجزء السفلي من النافذة الرئيسية لفتح نافذة **الدعم**.

   انقر فوق زر **أدوات الدعم**.
3. في نافذة **أدوات الدعم** التي يتم فتحها، انقر فوق زر **إنشاء تقرير حالة النظام**.

يتم إنشاء تقرير حالة النظام بالتنسيقين HTML وXML ويتم حفظه في الأرشيف sysinfo.zip. وبمجرد الانتهاء من عملية جمع المعلومات، بإمكانك عرض التقرير.

لعرض التقرير:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق ارتباط **الدعم** في الجزء السفلي من النافذة الرئيسية لفتح نافذة **الدعم**.

   انقر فوق زر **أدوات الدعم**.
3. في نافذة **أدوات الدعم** التي يتم فتحها، انقر فوق زر **عرض تقرير**.

4. افتح الأرشيف sysinfo.zip الذي يحتوى على ملفات التقرير.

تجميع بيانات فنية حول أداء التطبيق

يمكنك استخدام وظيفة تسجيل الأحداث لتجميع بيانات فنية حول أداء التطبيق ونظام التشغيل. تُمكِّن تقارير الأحداث المسجلة متخصصي خدمة الدعم الفني من تحليل المشكلة التي حدثت أثناء تشغيل التطبيق.

لتجميع معلومات حول مشكلة في تشغيل التطبيق وحفظ هذه المعلومات:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق ارتباط **الدعم** في الجزء السفلي من النافذة الرئيسية لفتح نافذة **الدعم**.
3. في نافذة **الدعم**، انقر فوق زر **أدوات الدعم**.
4. في قسم **أدوات الدعم**، حدد مستوى أهمية الأحداث من القائمة المنسدلة **مستوى التتبع**.

يمكنك تحديد مستويات الأهمية التالية للأحداث المسجلة في التقرير:

- مهم. يملأ برنامج Kaspersky PURE التقرير بمعلومات ول الأحداث التي ربما تكون مهمة لأمان الكمبيوتر، مثل اكتشاف كائن محتمل إصابته أو نشاط مشكوك فيه بالنظام.
- مستحسن. يملأ برنامج Kaspersky PURE التقرير بمعلومات حول الأحداث المهمة، إلى جانب الأحداث التي لا تمثل أهمية أولية في أمان الكمبيوتر.
- الكل. يقوم برنامج Kaspersky PURE بإنشاء تقرير مفصل حول كل الأحداث التي يمكن استخدامها لتشخيصات التطبيق.

5. لبدء عملية تسجيل الأحداث، انقر فوق زر **تمكين التتبعات**.
6. انقر فوق نافذة **الدعم**، وأعد تمثيل الموقف الذي واجه فيه التطبيق المشكلة.
7. بعد إعادة تمثيل الموقف، ارجع إلى قسم **أدوات الدعم**، وانقر فوق زر **تعطيل التتبعات** في نافذة **الدعم**.

يتوقف Kaspersky PURE عن تسجيل المعلومات الفنية حول أداء التطبيق ونظام التشغيل بأكمله.

بعد تجميع المعلومات الفنية حول أداء التطبيق، يمكنك إرسال البيانات المجمعة إلى خدمة دعم Kaspersky Lab الفني.

إرسال ملفات البيانات

بعد تجميع البيانات الفنية حول أداء التطبيق وإنشاء تقرير حالة النظام، يجب إرسالها إلى خبراء الدعم الفني في Kaspersky Lab.

وسوف تكون بحاجة إلى رقم طلب لرفع ملفات البيانات إلى خادم الدعم الفني. يوجد هذا الرقم في حسابي في Kaspersky على موقع الدعم الفني على الويب إذا كان طلبك نشطًا.

لتحميل ملفات البيانات إلى خادم الدعم الفني:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **الدعم** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق زر **أدوات الدعم**.

سيتم فتح النافذة **أدوات الدعم**.

4. في النافذة التي سيتم فتحها، انقر فوق زر **إرسال بيانات الخدمة إلى الدعم الفني**.

ومن ثم تفتح نافذة **إرسال تقرير**.

5. حدد خانات الاختيار الموجودة بجانب ملفات التتبع التي ترغب في إرسالها إلى خدمة الدعم الفني، ثم انقر فوق زر **إرسال**.

تفتح النافذة **أدخل رقم الطلب**.

6. حدد الرقم الذي تم تحديده لطلبك عبر الاتصال بخدمة الدعم الفني من خلال حسابي في Kaspersky، ثم انقر فوق زر **موافق**.

يتم حزم ملفات التتبع المحددة وإرسالها إلى خادم خدمة الدعم.

إذا تعذر عليك الاتصال بالدعم الفني لأي سبب، فإنه يمكن تخزين ملفات البيانات على الكمبيوتر الخاص بك ومن ثم إرسالها بعد ذلك من حسابي في Kaspersky.

لحفظ ملفات البيانات على القرص:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **الدعم** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق زر **أدوات الدعم**.
4. سيتم فتح النافذة **أدوات الدعم**.
5. في النافذة التي سيتم فتحها، انقر فوق زر **إرسال بيانات الخدمة إلى الدعم الفني**.

ومن ثم تفتح نافذة **إرسال تقرير**.

6. حدد خانات الاختيار الموجودة بجانب ملفات التتبع التي ترغب في إرسالها إلى خدمة الدعم الفني، ثم انقر فوق زر **إرسال**.

تفتح النافذة **أدخل رقم الطلب**.

7. انقر فوق زر **إلغاء الأمر** وأكد حفظ الملفات الموجودة على القرص عن طريق النقر فوق الزر **نعم** الموجود في النافذة التي سيتم فتحها.

ستفتح نافذة حفظ الأرشيف.

8. حدد اسم الأرشيف ثم أكد الحفظ.

يمكن إرسال الأرشيف الذي تم إنشاؤه إلى الدعم الفني من حسابي في Kaspersky.

تنفيذ البرنامج النصي لـ AVZ

نصح بعدم تغيير نص البرنامج النصي AVZ الذي استلمته من خبراء Kaspersky Lab. في حالة حدوث مشكلة أثناء تنفيذ البرنامج النصي، اتصل بالدعم الفني (راجع القسم "الحصول على دعم فني عبر الهاتف" على الصفحة 79).

لتشغيل برنامج AVZ النصي:

1. افتح نافذة التطبيق الرئيسية.
2. انقر فوق الارتباط **الدعم** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة **الدعم**.
3. في النافذة التي ستفتح، انقر فوق زر **أدوات الدعم**.

   سيتم فتح النافذة **أدوات الدعم**.
4. في النافذة التي يتم فتحها، انقر فوق زر **تشغيل البرنامج النصي**.

   سيتم فتح النافذة **تنفيذ برنامج AVZ النصي**.
5. انسخ النص من البرنامج النصي المرسل بواسطة المتخصصين في خدمة الدعم الفن، وألصقه في حقل الإدخال في النافذة التي ستفتح وانقر فوق زر **التالي**.

   سيتم تشغيل البرنامج النصي.

في حالة نجاح تنفيذ البرنامج النصي، يتم إغلاق المعالج. في حالة حدوث خطأ خلال تنفيذ البرنامج النصي، يعرض المعالج رسالة مقابلة.

المصطلحات

R

ROOTKIT

برنامج أو مجموعة من البرامج لإخفاء تتبع مهاجم أو برنامج ضار في نظام التشغيل.

في أنظمة التشغيل التي تعتمد على Windows، عادة يعني فيروس الجذر برنامج يخترق نظام التشغيل ويقاطع وظائف النظام (Windows API). وقبل كل شيء، فإن اعتراض وظائف API ذات المستوى المنخفض وتعديلها يتيح لمثل هذا البرنامج إيجاد نفسه في نظام التشغيل بشكل متخفٍ تمامًا. بإمكان فيروس الجذر في الغالب أيضًا أن يخفي وجود عمليات ومجلدات وملفات مخزنة على محرك أقراص، بالإضافة إلى مفاتيح التسجيل، وذلك إذا ما تم وصف هذه الأشياء في تكوين فيروس الجذر. والعديد من فيروسات الجذور تقوم بتثبيت برامج تشغيل وخدمات خاصة بها هي على نظام التشغيل (حيث تكون هذه الخدمات أيضًا "غير مرئية").

ا

الاحتيال

نوع من الاحتيال عبر الإنترنت الذي يتكون من خلال إرسال رسائل البريد الإلكتروني بغرض سرقة المعلومات السرية، عادة في شكل بيانات مالية.

الاستعادة

تغيير موقع الكائن الأصلي من العزل أو النسخ الاحتياطي إلى المجلد الأصلي الخاص به حيث كان يتم تخزين الكائن قبل أن يتم عزله أو تنظيفه أو حذفه، أو إلى مجلد معرف بواسطة المستخدم.

إعدادات البرنامج

إعدادات التطبيق العامة لكل أنواع المهام، والتي تنظم تشغيل التطبيق ككل، مثل إعدادات أداء التطبيق، وإعدادات التقرير، وإعدادات العزل.

إعدادات المهام

إعدادات تشغيل التطبيق الخاصة بكل نوع من أنواع المهام.

ب

بريد إلكتروني يُحتمل أن يكون غير مرغوب فيه

هي رسالة لا يمكن اعتبارها دون شك بريدًا إلكترونيًا غير مرغوب فيه، لكنها تشتمل على سمات عديدة من سمات البريد الإلكتروني غير المرغوب فيه (على سبيل المثال، بعض أنواع المراسلات والرسائل الإعلانية).

بروتوكول الإنترنت (IP)

البروتوكول الأساسي للإنترنت، يتم استخدامه بدون تغيير منذ وقت تطويره عام 1974. ويقوم بتنفيذ عمليات أساسية لنقل البيانات من كمبيوتر إلى آخر ويخدم كأساس للبروتوكولات الأعلى في المستوى مثل TCP و UDP. وهو يدير الاتصال ومعالجة الخطأ. وتتيح تقنيات مثل NST والتقنيع إخفاء عدد كبير من الشبكات الخاصة باستخدام عدد صغير من عناوين بروتوكول الإنترنت (أو حتى عنوان واحد)، مما يتيح الاستجابة لطلبات الإنترنت دائمة التزايد باستخدام مساحة عنوان IPv4 محدودة.

البرنامج النصي

برنامج كمبيوتر صغير أو جزء مستقل من برنامج (وظيفة)، والذي يتم تطويره، كقاعدة، لتنفيذ مهمة معينة. ويستخدم غالباً مع البرامج المضمنة في النص التشعبي. وتعمل البرامج النصية عند فتح مواقع ويب معينة على سبيل المثال.

إذا تم تمكين الحماية في الوقت الحقيقي، يقوم التطبيق بتتبع بدء تشغيل البرامج النصية واعتراضها وفحصها للبحث عن الفيروسات. ووفقاً لنتائج الفحص، يمكنك منع تنفيذ برنامج نصي أو السماح بذلك.

البريد الإلكتروني غير المرغوب فيه

غالباً ما تحتوي كميات ضخمة من رسائل البريد الإلكتروني غير المرغوب فيها على رسائل دعائية.

ت

تحديث

إجراء استبدال/إضافة ملفات جديدة (قواعد بيانات أو وحدات تطبيق) تم استردادها من خوادم تحديث Kaspersky Lab.

التحديث المتاح

حزمة من التحديثات الخاصة بالوحدات النمطية لتطبيق Kaspersky Lab وتتضمن مجموعة من الحزم الطارئة التي يتم تحريرها أثناء فترة زمنية محددة، والتعديلات التي تتم على هيكل التطبيق.

تحديث عاجلة

تحديثات هامة لوحدات تطبيق Kaspersky Lab.

تحديث قاعدة بيانات

وظيفة يقوم بها تطبيق Kaspersky Lab تتيح له الحفاظ على الحماية في حالة حديثة. أثناء التحديث، يقوم التطبيق بتنزيل التحديثات الخاصة بقواعد البيانات والوحدات النمطية الخاصة به من خوادم تحديث Kaspersky Lab وتثبيتها وتطبيقها تلقائيًا.

تطبيق غير متوافق

تطبيق مكافحة فيروسات من تطوير طرف ثالث أو أن تطبيق Kaspersky Lab لا يدعم الإدارة عبر Kaspersky PURE.

تقنية iChecker

تقنية تسمح بزيارة سرعة عمليات الفحص لمكافحة الفيروسات من خلال استثناء الكائنات التي لم تتغير منذ آخر مرة تم فحصها، بشرط عدم تعديل معلمات الفحص (قواعد البيانات والإعدادات). ويتم تخزين المعلومات الخاصة بكل ملف في قاعدة بيانات خاصة. ويتم استخدام هذه التقنية في كل من الحماية في الوقت الفعلي وأوضاع الفحص عند الطلب.

على سبيل المثال، لديك ملف أرشيف تم فحصه بواسطة تطبيق Kaspersky Lab وتعيين غير مصاب له. في المرة القادمة سيقوم التطبيق بتخطي هذا الأرشيف ما لم يتم تنبيه التطبيق أو ما لم يتم تغيير إعدادات الفحص. وإذا قمت بتغيير محتوى الأرشيف بإضافة كائن جديد إليه، أو تعديل إعدادات الفحص، أو تحديث قواعد بيانات التطبيق، ستتم إعادة فحص الأرشيف.

ضوابط تقنية iChecker:

- لا تعمل هذه التقنية مع الملفات الكبيرة، حيث أنه من الأسرع فحص الملف بدلاً من التحقق مما إذا كان قد تم تعديله منذ آخر عملية فحص؛
- تدعم التقنية عددًا محدودًا من التنسيقات.

تنشيط التطبيق

تحويل التطبيق إلى وضع الوظائف الكاملة يتم تنفيذ تنشيط التطبيق بواسطة المستخدم أثناء التثبيت أو بعده. ينبغي أن يكون لدى المستخدم رمز تنشيط لتنشيط التطبيق.

التوقيع الرقمي

كتلة مشفرة من البيانات في مستند أو تطبيق. يتم استخدام التوقيع الرقمي لتحديد مؤلف المستند أو التطبيق. لإنشاء توقيع رقمي، يجب أن يمتلك مؤلف المستند أو التطبيق شهادة رقمية تؤكد هوية المؤلف.

يسمح لك التوقيع الرقمي بالتحقق من صحة مصدر البيانات وتكامل البيانات بالإضافة إلى حمايتك من التزوير.

تنظيف الكائنات عند إعادة التشغيل

طريقة لمعالجة الكائنات المصابة التي تستخدم بواسطة التطبيقات الأخرى في لحظة التنظيف. وهي تتكون من إنشاء نسخة من كائن مصاب، وتنظيف النسخة التي تم إنشاؤها، واستبدال الكائن الأصلي المصاب بالنسخة النظيفة بعد إعادة تشغيل النظام التالية.

تنظيف

طريقة لمعالجة الكائنات المصابة التي ينتج عنها وجود استعادة كاملة أو جزئية للبيانات. لا يمكن تنظيف جميع الكائنات المصابة.

ح

الحالة الإيجابية الخاطئة

هو موقف يعتبر فيه تطبيق Kaspersky Lab أحد الكائنات غير المصابة أنه كائن مصاب بسبب تشابه رمزه مع رمز أحد الفيروسات.

حالة الحماية

حالة الحماية الحالية، والتي تحدد مستوى أمان الكمبيوتر.

الحماية في الوقت الحقيقي

هو وضع تشغيل النظام الذي يتم فيه فحص الكائنات للبحث عن وجود رمز خبيث في الوقت الحقيقي.

يعترض التطبيق جميع محاولات فتح أي كائن (للقراءة أو للكتابة أو للتنفيذ) ويفحص الكائن بحثًا عن تهديدات. يتم ترك الكائنات غير المصابة للمستخدم، بينما تتم معالجة الكائنات المصابة أو المحتمل إصابتها وفقًا لإعدادات المهمة (تنظيفها أو إزالتها).

حاوية

كائن مشفر مصمم لتخزين البيانات السرية. تعتبر الخاوية عبارة عن محرك ظاهري قابل للإزالة تتم حمايته باستخدام كلمة المرور لتخزين الملفات والمجلدات.

ويجب تثبيت تطبيق Kaspersky PURE على الكمبيوتر لكي تتوفر وظائف الحاوية.

حماية المستعرض

يتم بدء تشغيل المستعرض في وضع الخدمات النقدية الآمنة. يتم بدء تشغيل وضع التشغيل الآمن لمواقع الويب عندما تقوم بزيارة موقع ويب لخدمات بنكية على الإنترنت من أجل حماية بيانات المستخدم من السرقة. في هذه الحالة، يعرض المستعرض القياسي - المستخدم للوصول إلى موقع الويب - رسالة تخبرك ببدء تشغيل حماية المستعرض.

حذف الرسائل

طريقة معالجة رسالة البريد الإلكتروني التي يتم خلالها إزالة الرسالة فعليًا. نحن نوصي بتطبيق هذه الطريقة على الرسائل التي تحتوي على بريد إلكتروني غير مرغوب فيه بصورة واضحة أو برامج ضارة. قبل حذف أية رسالة، يتم حفظ نسخة منها في العزل (هذا ما لم يتم تعطيل هذا الخيار).

حذف كائن

طريقة معالجة الكائنات التي تنتهي بحذفها ماديًا من موقعها الأصلي (قرص ثابت، مجلد، مورد شبكة اتصال). ونوصي بتطبيق هذه الطريقة على الكائنات الخطرة التي يتعذر تنظيفها لأي سبب.

حزمة التحديث

حزمة ملف خاصة بتحديث الوحدات النمطية للتطبيق. أحد تطبيقات Kaspersky Lab يقوم بنسخ حزم التحديث من خوادم تحديث Kaspersky Lab وتثبيتها وتطبيقها بشكل تلقائي.

خ

خدمة اسم المجال (DNS)

نظام موزع لتحويل اسم مضيف (كمبيوتر أو جهاز شبكة آخر) إلى عنوان بروتوكول إنترنت. ويعمل DNS على شبكات TCP/IP. كحالة خاصة، يستطيع DNS تخزين ومعالجة الطلبات العكسية، من خلال تحديد اسم مضيف عن طريق عنوان بروتوكول الإنترنت الخاص به (سجل PTR). يتم تنفيذ تحليل أسماء DNS عادة بواسطة تطبيقات الشبكة، وليس المستخدمين.

الخدمات النقدية الآمنة

هي وحدة نمطية للتطبيق تحمي البيانات السرية التي يقوم المستخدم بإدخالها على مواقع الويب الخاصة بالخدمات البنكية أو الخدمات النقدية الإلكترونية، كما أنها تحول دون سرقة النقود خلال عمليات الدفع على الإنترنت.

خطورة الحدث

تمت مواجهة خاصية من خصائص الحدث أثناء تشغيل تطبيق Kaspersky Lab. هناك أربعة مستويات من الخطورة:

- حدث حرج.
- خطأ.
- تحذير.
- معلومات.

قد توجد أحداث بنفس النوع من مستويات الخطورة المختلفة تبعًا للموقف الذي وقع فيه الحدث.

خوادم تحديث KASPERSKY LAB

خوادم Kaspersky Lab HTTP التي يتم رفع قواعد بيانات مكافحة الفيروسات المحدثة والوحدات النمطية للتطبيق إليها.

رأس

المعلومات في بداية ملف أو رسالة، والتي تتكون من بيانات منخفضة المستوى في حالة ملف (أو رسالة) ومعالجته. وعلى وجه الخصوص، يحتوي رأس رسالة البريد الإلكتروني على بيانات مثل المعلومات حول المرسل والمستلم والتاريخ.

راصد لوحة المفاتيح

مكون فرعي للتطبيق المسئول عن فحص أنواع معينة من البريد الإلكتروني. وتتوقف مجموعة المعترضات المحددة لعملية التثبيت الخاصة بك على دور أو توليفة أدوار التطبيق التي يتم نشرها.

الرسالة غير المناسبة

هي رسالة بريد إلكتروني تحتوي على لغة مسيئة.

ش

شبكة أمان KASPERSKY (KSN)

بنية أساسية من خدمات الإنترنت التي توفر الوصول إلى قاعدة معلومات Kaspersky Lab عبر الإنترنت التي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. إن استخدام البيانات من شبكة أمان Kaspersky يضمن الاستجابة بشكل أسرع من قِبل تطبيقات Kaspersky Lab للتهديدات غير المعروفة، كما أنه يُحسِّن من كفاءة بعض مكونات الحماية، ويقلل أيضًا من مخاطر الحالات الإيجابية الخاطئة.

ع

العزل

مخزن مخصص يضع فيه التطبيق نُسخًا احتياطية من الملفات التي تم تعديلها أو حذفها أثناء عملية التنظيف. يتم تخزين نُسخ الملفات بتنسيق خاص لا يمثل تهديدًا على الكمبيوتر.

ف

فترة الترخيص

الفترة الزمنية التي يمكنك خلالها الوصول إلى ميزات التطبيق والحقوق الخاصة به لاستخدام الخدمات الإضافية.

فحص الحركة

هو فحص فوري يستخدم معلومات من الإصدار الحالي (أحدث إصدار) من قواعد البيانات للكائنات المنقولة عبر جميع البروتوكولات (مثل HTTP، وFTP، إلخ).

فيروس غير معروف

فيروس جديد لم يتم تسجيله حتى الآن في قواعد البيانات. يتحقق التطبيق عادة من الفيروسات غير المعروفة في الكائنات بواسطة المحلل المساعد على الاكتشاف. يتم وضع تسميت لتلك الكائنات باعتبارها محتملة الإصابة.

ق

قاعدة بيانات عناوين الويب الخبيثة

قائمة بعناوين ويب التي تشتمل على محتوى يمكن اعتباره خطرًا. تم إنشاء القائمة بواسطة خبراء Kaspersky Lab. ويتم تحديثها بصفة منتظمة ويتم تضمينها في حزمة تطبيق Kaspersky Lab.

قاعدة بيانات عناوين الويب الاحتيالية

قائمة بعناوين الويب التي يتم تعريفها كعناوين احتيالية بواسطة خبراء Kaspersky Lab. يتم تحديث قاعدة البيانات بانتظام، كما أنها تمثل جزءًا من تطبيق Kaspersky Lab.

قناع الشبكة الفرعية

يقوم قناع الشبكة الفرعية (الذي يعرف أيضًا بقناع الشبكة) وعنوان شبكة الاتصال بتحديد عناوين أجهزة الكمبيوتر الموجودة على الشبكة.

قواعد البيانات

قواعد البيانات التي تحتوي على معلومات حول تهديدات الأمان الخاصة بالكمبيوتر والمعروفة لـ Kaspersky Lab وقت إصدار قواعد البيانات. تسمح السجلات التي يتم تضمينها في قواعد البيانات باكتشاف الرموز البرمجية الخبيثة في الكائنات التي تم فحصها. يتم إنشاء قواعد البيانات بواسطة خبراء Kaspersky Lab ويتم تحديثها على مدار الساعة.

قطاع تمهيد القرص

قطاع التمهيد هو منطقة معينة على القرص الثابت لجهاز كمبيوتر أو قرص مرن أو وسيط تخزين بيانات آخر. وهو يحتوي على معلومات حول نظام ملفات القرص وبرنامج محمل التمهيد المسئول عن بدء نظام التشغيل.

وهناك عدد من الفيروسات التي تصيب قطاعات التمهيد، والتي يطلق عليها لذلك فيروسات التمهيد. ويسمح تطبيق Kaspersky Lab بفحص قطاعات التمهيد للبحث عن الفيروسات وتنظيفها في حالة العثور على إصابة.

قناع الملف

تمثيل لاسم الملف باستخدام أحرف البدل. أحرف البدل القياسية المستخدمة في أقنعة الملف هي * و ? حيث تمثل النجمة * أي عدد من الحروف بينما تشير علامة الاستفهام ? إلى أي حرف مفرد.

ك

كلمة المرور الرئيسية

كلمة مرور واحدة تحمي قاعدة بيانات إدارة كلمات المرور وتوفر لك الوصول إلى البيانات.

كائن مصاب

كائن مقطع من رمزه مطابق تمامًا لجزء من تهديد معروف. لا توصي Kaspersky Lab باستخدام مثل هذه الكائنات.

كائن يحتمل كونه مصابًا

هو كائن يشمل رمزه على مقطع مُعدَّل من رمز برمجيات خبيثة معروفة، أو كائن يمثل هذه البرمجيات الخبيثة من خلال سلوكه.

كائنات بدء التشغيل

مجموعة من التطبيقات اللازمة لبدء تشغيل وتصحيح عمل نظام التشغيل والبرامج الموجودة على جهاز الكمبيوتر. يتم تنفيذ هذه الكائنات في كل مرة يبدأ فيها نظام التشغيل. هناك فيروسات قادة على إصابة كائنات بدء التشغيل على وجه الخصوص، وهو ما قد يحول دون تحميل نظام التشغيل.

م

المهمة

الوظائف التي يقوم بها تطبيق Kaspersky Lab يتم تنفيذها كمهام، مثل: حماية الملف في الوقت الحقيقي، فحص كامل الكمبيوتر، تحديث قاعدة البيانات.

مخزن الإنترنت

طريقة لتخزين البيانات على خوادم بعيدةً عادةً ما تكون موزعة جغرافيًا. ويفضي التخزين على الإنترنت البساطة على عملية المزامنة بين أجهزة الكبيوتر والأجهزة المحمولة المختلفة. ويلزم توفر اتصال بالإنترنت لاستخدام التخزين على الإنترنت.

مجلد النسخ الاحتياطي

مساحة على القرص أو محرك قابل للإزالة محدد لإنشاء نُسخ احتياطية من الملفات أثناء مهام النسخ الاحتياطي.

مستوى التهديد

فهرس يوضح مدى احتمال أن يمثل أحد التطبيقات تهديدًا على نظام التشغيل. يتم حساب مستوى التهديد باستخدام التحليل المساعد على الاكتشاف وفقًا لنوعين من المعايير:

- ثابت (مثل معلومات حول ملف تشغيل أحد التطبيقات: الحجم، وتاريخ الإنشاء، إلخ.)؛
- ديناميكي، يتم الاستخدام أثناء تحفيز تشغيل التطبيق في بيئة ظاهرية (تحليل طلبات التطبيق لوظائف النظام).

يسمح مستوى التهديد باكتشاف أي سلوك مطابق للبرمجيات الخبيثة. كلما انخفض مستوى التهديد، زادت الإجراءات التي سيُسمح للتطبيق القيام بها في النظام.

مستوى الأمان

يتم تعريف مستوى الأمان كمجموعة سابقة التحديد من الإعدادات لأحد مكونات التطبيقات.

المحلل المساعد على الاكتشاف

تقنية لاكتشاف معلومات التهديدات التي لم يتم إضافتها حتى الآن إلى قواعد بيانات Kaspersky Lab. يتيح المحلل المساعد على الاكتشاف اكتشاف الكائنات التي تعمل بطريقة قد تمثل تهديدًا لأمان الكمبيوتر. يتم اعتبار الكائنات التي تم اكتشافها بواسطة المحلل المساعد على الاكتشاف على أنها محتملة الإصابة. على سبيل المثال، يمكن اعتبار أحد الكائنات محتملة الإصابة إذا كانت تحتوي على تسلسلات من الأوامر التي تتطابق مع الكائنات الخبيثة (فتح الملف، الكتابة إلى ملف).

منع كائن

رفض الوصول إلى كائن من التطبيقات الخارجية. ولا يمكن قراءة أي كائن ممنوع أو تنفيذه أو تغييره أو حذفه.

ملف مضغوط

ملف أرشيف يحتوي على برنامج إلغاء ضغط وتعليمات لنظام التشغيل لتنفيذه.

ن

انتشار الفيروسات

سلسلة من المحاولات المتعمدة لإصابة الكمبيوتر بفيروس.

و

الوحدات النمطية للتطبيق

الملفات الموجودة في حزمة تثبيت Kaspersky Lab المسؤولة عن تنفيذ مهامها الرئيسية. وتتوافق وحدة نمطية تشغيلية معينة مع كل نوع مهمة يتم تنفيذها بواسطة التطبيق (الحماية الفورية، الفحص عند الطلب، التحديثات). ومن خلال تشغيل فحص كامل لجهاز الكمبيوتر من النافذة الرئيسية، ستقوم ببدء تنفيذ وحدة المهمة هذه.

KASPERSKY LAB ZAO

تحظى برامج Kaspersky Lab بشهرة عالمية كبيرة لحمايتها ضد الفيروسات، والبرمجيات الخبيثة، والبريد الإلكتروني غير المرغوب فيه، وهجمات الشبكة والمتسللين، والتهديدات الأخرى.

في عام 2008، تم تصنيف Kaspersky Lab بين أعلى أربعة موردين على مستوى العالم متخصصين في توريد حلول برامج أمان المعلومات للمستخدمين النهائيين (IDC Worldwide Endpoint Security Revenue by Vendor). كما تعتبر Kaspersky Lab من المطورين المفضلين لأنظمة حماية الكمبيوتر بين المستخدمين في المنازل في روسيا، وذلك وفق استطلاع COMCON "TGI-Russia 2009".

تم تأسيس Kaspersky Lab في روسيا في عام 1997. وتتكون اليوم من مجموعة عالمية من الشركات التي اتخذت من موسكو مقرًا لها وتتألف من خمسة فروع إقليمية تقوم بإدارة أنشطة الشركة في روسيا، وأوروبا الشرقية والغربية، والشرق الأوسط، وإفريقيا، وأمريكا الشمالية والجنوبية، واليابان والصين والدول الأخرى في منطقة المحيط الهادي الأسيوية. ويعمل تحت إمرتها أكثر من 2000 موظف من المتخصصين المؤهلين.

المنتجات. توفر منتجات Kaspersky Lab الحماية لجميع الأنظمة - من أجهزة الكمبيوتر المنزلية إلى شبكات الشركات الكبيرة.

ويتضمن نطاق المنتجات الشخصي تطبيقات مكافحة الفيروسات لسطح المكتب والكمبيوتر المحمول وأجهزة الكمبيوتر اللوحي والهواتف الذكية وأجهزة الهواتف الجوالة الأخرى.

ويوفر Kaspersky Lab تطبيقات وخدمات لحماية محطات العمل والملفات وخوادم الويب وعبارات البريد وجدران الحماية. وعن طريق الاستخدام المشترك مع نظام الإدارة المركزية لـ Kaspersky Lab، فإن هذه الحلول تضمن وجود حماية فعالة تلقائية للشركات والمنظمات ضد التهديدات الموجهه لأجهزة الكمبيوتر. ولقد تم اعتماد منتجات Kaspersky Lab بواسطة كبرى معامل الاختبار وتتوافق مع البرامج الخاصة بالكثير من موردي تطبيقات الكمبيوتر كما تم تحسينها ليتم تشغيلها على الكثير من الأنظمة الأساسية للأجهزة.

ويعمل محللو الفيروسات في Kaspersky Lab على مدار الساعة. حيث يعثرون كل يوم على المئات من التهديدات الجديدة الموجهة لأجهزة الكمبيوتر، ويقومون بإنشاء أدوات لاكتشافها وتنظيفها، وإضافتها إلى قواعد البيانات التي تستخدمها تطبيقات Kaspersky Lab. *يتم تحديث قاعدة بيانات Kaspersky Lab لمكافحة الفيروسات كل ساعة وقاعدة بيانات مكافحة البريد الإلكتروني غير المرغوب فيه –كل خمس دقائق.*

التقنيات. لقد تم تطوير العديد من التقنيات التي تعد الآن جزءا لا يتجزأ من أدوات مكافحة الفيروسات الحديثة من قبل Kaspersky Lab. ولا يعتبر الأمر صدفة أن الكثير من المطورين الآخرين يستخدمون مؤشر Kernel لمكافحة الفيروسات من Kaspersky في منتجاتهم، بما في ذلك: Safenet (الولايات المتحدة الأمريكية)، و Alt-N (الولايات المتحدة الأمريكية)، وBlue Coat Systems (الولايات المتحدة الأمريكية), Check Point Software Technologies (إسرائيل)، Clearswift (المملكة المتحدة)، و Communigate Systems (الولايات المتحدة الأمريكية)، وCritical Path (أيرلندا)، D-Link (تايوان)، M86 Security (الولايات المتحدة الأمريكية)، وGFI (مالطا)، وIBM (الولايات المتحدة الأمريكية)، Juniper Networks (الولايات المتحدة الأمريكية), LANDesk (الولايات المتحدة الأمريكية)، Microsoft (الولايات المتحدة الأمريكية)، وNETASQ (فرنسا)، NETGEAR (الولايات المتحدة الأمريكية)، Parallels (روسيا)، وSonicWALL (الولايات المتحدة الأمريكية)، WatchGuard Technologies (الولايات المتحدة الأمريكية)، ZyXEL Communications (تايوان). ولقد تم الحصول على براءات اختراع للكثير من التقنيات التي ابتكرتها الشركة.

الإنجازات. عبر سنوات طويلة، فازت شركة Kaspersky Lab بمئات الجوائز نظير خدماتها في مكافحة تهديدات الكمبيوتر. على سبيل المثال، ففي عام 2010 فازت Kaspersky لمكافحة الفيروسات بالعديد من الجوائز المتقدمة في اختبار تم تحت إشراف AV-Comparatives، وهو معمل شهير معتمد في النمسا متخصص في مكافحة الفيروسات. ولكن يتمثل الإنجاز الرئيسي لشركة Kaspersky Lab في ولاء مستخدميه في جميع أنحاء العالم. حيث تحمي منتجات وتقنيات الشركة أكثر من 300 مليون مستخدم، ويزيد عدد عملاء الشركة عن 200000 عميل.

الموقع الرسمي لشركة Kaspersky Lab:	http://me.kaspersky.com
موسوعة الفيروسات:	http://www.securelist.com
مختبر مكافحة الفيروسات:	newvirus@kaspersky.com (مخصص فقط لإرسال الملفات محتملة الإصابة في تنسيق الأرشيف) http://support.kaspersky.com/virlab/helpdesk.html (للاستعلامات الموجهة إلى محللي الفيروسات)
منتدى ويب Kaspersky Lab:	http://forum.kaspersky.com

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يتم تضمين معلومات حول رمز الطرف الخارجي في ملف باسم legal_notices.txt في مجلد تثبيت التطبيق.

إشعارات العلامة التجارية

العلامات التجارية المسجلة وعلامات الخدمة مملوكة لأصحابها.

يعتبر Google Chrome علامة تجارية مملوكة لشركة Google, Inc.

تعتبر Intel وPentium وAtom علامات تجارية لشركة Intel Corporation مسجلة في الولايات المتحدة الأمريكية وأي مكان آخر.

تعد كل من Microsoft وWindows وWindows Vista وInternet Explorer علامات تجارية مملوكة لشركة Microsoft Corporation ومسجلة في الولايات المتحدة الأمريكية والبلدان الأخرى.

يعتبر كل من Mozilla و Firefox علامات تجارية لشركة Mozilla.

الفهرس

K

ا

أ

إ

ا

ت