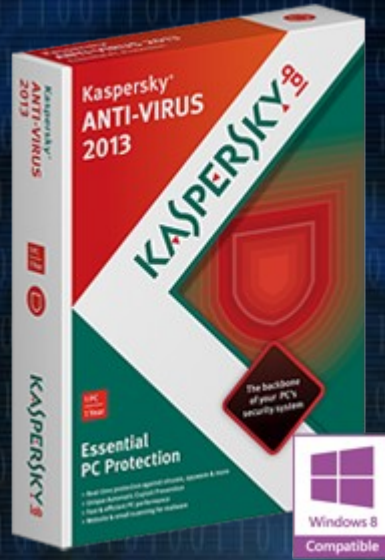


دليل المستخدم لبرنامج مقاومة الفيروسات كاسبرسكى أنتى فايروس 2013



Kaspersky Anti-Virus 2013

اعداد
شريف م. عوض

برعاية موقع كاش العرب

طريقك إلى العمل الجاد

www.Cash4Arab.com

Kaspersky Anti-Virus 2013

KASPERSKY ^{lab}

المستخدم ليل

إصدار ال تطب يق 13.0

عزيزي المستخدم،

نشكركم لاختيار منتجنا. نأمل في أن تجد هذه الوثائق مفيدة وأنها ستوفر إجابات لمعظم الأسئلة التي قد تظهر.

انتباه! ترجع ملكية هذه الوثيقة إلى شركة Kaspersky Lab ZAO (يشار إليها فيما بعد في هذا المستند بـ Kaspersky Lab) وجميع الحقوق المتعلقة بهذه الوثيقة محفوظة بموجب قوانين حقوق التأليف والنشر الخاصة بروسيا الاتحادية والمعاهدات الدولية. ويؤدي النسخ والتوزيع غير القانوني لهذه الوثيقة أو لأجزاء منها إلى التعرض للمساءلة المدنية أو الإدارية أو الجنائية بمقتضى القانون المعمول به.

لا يُسمح بأية طريقة من طرق النسخ أو التوزيع لأية مواد، بما في ذلك الترجمة، إلا بإذن كتابي من Kaspersky Lab.

يقتصر استخدام هذه الوثيقة وكذلك الصور الرسومية الموجودة بها على أغراض الحصول على معلومات أو على أغراض غير تجارية أو شخصية فحسب.

يجوز تعديل هذه الوثيقة دون إخطار مسبق. يمكنك العثور على أحدث إصدار من هذه الوثيقة على موقع ويب Kaspersky Lab بالعنوان التالي <http://www.kaspersky.com/docs>.

لا تتحمل Kaspersky Lab أية مسؤولية قانونية تتعلق بمحتوى أو جودة أو ملائمة أو دقة أية مواد مستخدمة في هذه الوثيقة، والتي تُحفظ حقوقها لأطراف ثالثة، كما لا تتحمل المسؤولية عن أية أضرار محتملة تصاحب استخدام هذه الوثيقة.

تاريخ مراجعة المستند: 8/7/2012

© 2012 Kaspersky Lab ZAO. جميع الحقوق محفوظة.

<http://www.kaspersky.com>
<http://support.kaspersky.com>

المحتويات

6	حول هذا الدليل
6	في هذا المستند
7	اصطلاحات الوثيقة
9	مصادر المعلومات المتعلقة بالتطبيق
9	مصادر معلومات البحث المستقل
10	مناقشة تطبيقات Kaspersky Lab في المنتدى
10	الاتصال بإدارة المبيعات
10	الاتصال بوحدة الكتابة الفنية والترجمة عن طريق البريد الإلكتروني
11	برنامج KASPERSKY ANTI-VIRUS
11	ما الجديد
11	حزمة التوزيع
12	ميزات التطبيق الأساسية
13	خدمة المستخدمين
13	متطلبات الأجهزة والبرامج
15	تنصيب التطبيق وإزالته
15	إجراء التنصيب القياسي
16	الخطوة 1. جاري البحث عن نسخة أحدث من التطبيق
16	الخطوة 2. بدء تثبيت التطبيق
16	الخطوة 3. مراجعة اتفاقية الترخيص
17	الخطوة 4. بيان تجميع بيانات شبكة أمان Kaspersky
17	الخطوة 5. التنصيب:
18	الخطوة 6. إكمال التنصيب
18	الخطوة 7. تنشيط التطبيق
18	الخطوة 8. تسجيل المستخدم
19	الخطوة 9. استكمال التفعيل
19	تحديث إلى الإصدار السابق من Kaspersky Anti-Virus
20	الخطوة 1. جاري البحث عن نسخة أحدث من التطبيق
20	الخطوة 2. بدء تثبيت التطبيق
20	الخطوة 3. مراجعة اتفاقية الترخيص
20	الخطوة 4. بيان تجميع بيانات شبكة أمان Kaspersky
21	الخطوة 5. التنصيب:
21	الخطوة 6. إكمال التنصيب
21	سيناريوهات التنصيب غير القياسية
22	إزالة التطبيق
22	الخطوة 1. حفظ البيانات لإعادة الاستخدام
23	الخطوة 2. تأكيد إزالة التطبيق
23	الخطوة 3. إزالة التطبيق. استكمال الإزالة
24	ترخيص التطبيق
24	حول اتفاقية ترخيص المستخدم النهائي
24	حول الترخيص
25	حول رمز التنشيط
25	حول تزويد البيانات
27	حل المهام النمطية
29	تنشيط التطبيق

30	الحصول على الترخيص وتجديده
30	إدارة إخطارات التطبيق
31	تقييم حالة حماية الكمبيوتر وحل موضوعات الأمان
32	تحديث قواعد البيانات ووحدات التطبيق
32	فحص المناطق الحرجة في الكمبيوتر الخاص بك للبحث عن الفيروسات
32	فحص كامل للكمبيوتر للبحث عن الفيروسات
33	فحص ملف أو مجلد أو قرص أو أي كائن آخر بحثًا عن الفيروسات
34	فحص الكائنات محتملة الإصابة
35	استعادة كائن تم حذفه أو تنظيفه بواسطة التطبيق
36	استعادة نظام التشغيل بعد الإصابة
38	فحص البريد الإلكتروني وتصفية مرفقات رسائل البريد الإلكتروني
39	فحص الكمبيوتر بحثًا عن الثغرات الأمنية
39	فحص سمعة التطبيق
40	حماية البيانات الشخصية ضد السرقة
41	الحماية ضد الاحتيال
42	لوحة المفاتيح الظاهرية
43	منظف الخصوصية
46	تقييم الحالة الآمنة لموقع الويب
47	استخدام ملف تعرف الألعاب لوضع ملء الشاشة
47	إنشاء قرص الإنقاذ واستخدامه
47	إنشاء قرص الإنقاذ
49	بدء تشغيل الكمبيوتر باستخدام قرص الإنقاذ
50	تقييد الوصول إلى برنامج Kaspersky Anti-Virus باستخدام كلمة المرور
51	إيقاف حماية الكمبيوتر واستعادتها
51	عرض تقرير تشغيل التطبيق
52	استعادة إعدادات التطبيق الافتراضية
54	استيراد إعدادات التطبيق إلى Kaspersky Anti-Virus المثبت على كمبيوتر آخر
54	استخدام أدوات Kaspersky الذكية
56	المشاركة في شبكة أمان (Kaspersky (KSN
56	تمكين المشاركة في شبكة أمان Kaspersky وتعطيلها
56	فحص الاتصال بشبكة أمان Kaspersky
57	كيفية التبديل من برنامج Kaspersky Anti-Virus إلى برنامج Kaspersky Internet Security
58	التبديل مؤقتًا إلى الإصدار التجريبي
59	التبديل إلى الإصدار التجاري
60	الاتصال بخدمة الدعم الفني
60	كيفية الحصول على الدعم الفني
60	الدعم الفني عبر الهاتف
60	الحصول على الدعم الفني من خلال حسابي في Kaspersky
62	استخدام ملف التتبع وبرنامج AVZ النصي
62	إنشاء تقرير حالة النظام
63	إرسال ملفات البيانات
64	تنفيذ البرنامج النصي لـ AVZ

65	المصطلحات
71	KASPERSKY LAB ZAO
73	معلومات حول التعليمات البرمجية الخاصة بطرف ثالث
73	إشعارات العلامة التجارية
74	الفهرس

حول هذا الدليل

هذا المستند عبارة عن دليل المستخدم لـ Kaspersky Anti-Virus.

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

يهدف هذا الدليل إلى تنفيذ ما يلي:

- مساعدتك على تثبيت Kaspersky Anti-Virus وتنشيطه واستخدامه.
- ضمان البحث السريع عن المعلومات حول المشكلات المتعلقة بالتطبيق.
- شرح مصادر المعلومات الأخرى المتعلقة بالتطبيق وطرق تلقي الدعم الفني.

في هذا القسم:

6. المستند هذا في

7. الوثيقة اصطلاحات

في هذا المستند

تحتوي هذه الوثيقة على الأقسام التالية.

مصادر المعلومات المتعلقة بالتطبيق

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

برنامج Kaspersky Anti-Virus

يصف هذا القسم ميزات التطبيق، كما أنه يوفر معلومات مختصرة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين في التطبيق. ويوفر هذا القسم معلومات 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

يتضمن هذا القسم معلومات حول المفاهيم الأساسية لتنشيط التطبيق. قم بقراءة هذا القسم لتتعرف على المزيد حول الهدف من اتفاقية الترخيص وأنواع التراخيص وطرق تنشيط التطبيق وتجديد الترخيص.

حل المهام النمطية

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.

المصطلحات

يحتوي هذا القسم على قائمة المصطلحات التي ترد في المستند وتعريفاتها.

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 والمستخدم في هذا المستند.

الفهرس

يسمح لك هذا القسم بالعثور السريع على المعلومات المطلوبة ضمن المستند.

اصطلاحات الوثيقة

تتم مصاحبة نص المستند بعناصر دلالية نوصيك بالانتباه الشديد له: التحذيرات والتلميحات والأمثلة.

يتم استخدام اصطلاحات الوثيقة لتمييز العناصر الدلالية. يوضح الجدول التالي الاتفاقيات والأمثلة الخاصة باستخدامها.

1. Table. 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.
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 فوق خلفية صفراء تحت العنوان "مثال".

وصف اصطلاح الوثيقة	نص عينة
<p>يتم كتابة العناصر الدلالية التالية بالخط المائل في النص:</p> <ul style="list-style-type: none"> المصطلحات الجديدة أسماء حالات وأحداث التطبيق 	<p>تحديث يعني... قواعد البيانات قديمة وقوع حدث.</p>
<p>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.</p>	<p>اضغط إدخال. اضغط على ALT+F4.</p>
<p>يتم تمييز أسماء عناصر واجهة التطبيق، مثل حقول الإدخال وعناصر القائمة والأزرار بالخط العريض.</p>	<p>انقر فوق الزر تمكين.</p>
<p>يتم كتابة العبارات الافتتاحية في التعليمات بحروف مائلة وتكون مصحوبة بعلامة سهم.</p>	<p>► لتكوين جدول المهمة:</p>
<p>يتم تمييز الأنواع التالية من المحتوى النصي بكتابتها بخط خاص:</p> <ul style="list-style-type: none"> نص في سطر الأوامر نص الرسائل الذي يعرضه التطبيق على الشاشة البيانات التي يجب أن يدخلها المستخدم. 	<p>في سطر الأوامر، اكتب تعليمات. ستظهر بعد ذلك الرسالة التالية: حدد التاريخ بتنسيق يوم / شهر / سنة .</p>
<p>يتم وضع المتغيرات داخل أقواس زاوية بدلاً من المتغير، قم بإدراج القيمة المقابلة، مع عدم تضمين أقواس الزاوية.</p>	<p><اسم المستخدم></p>

مصادر المعلومات المتعلقة بالتطبيق

يصف هذا القسم مصادر المعلومات الخاصة بالتطبيق ويسرد مواقع الويب التي يمكنك استخدامها لمناقشة تشغيل التطبيق. يمكنك اختيار أنسب مصدر معلومات، وفقاً لمستوى ضرورة وأهمية الموضوع الخاص بك.

في هذا القسم:

- 9.المستقل البحث معلومات م صادر
- 10.المندى في Kaspersky Lab تطبيقات مناقشة
- 10.المبيعات بإدارة الاتصال
- 10.الإلكتروني البريد طريق عن والترجمة الفنية الكتابة وحدة الاتصال

مصادر معلومات البحث المستقل

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، نوصيك بالاتصال بالدعم الفني لـ Kaspersky Lab (راجع القسم "الإعدادات عبر الإنترنت" على الصفحة 60).

يجب توفر اتصالاً بالإنترنت لتتمكن من استخدام مصادر المعلومات الموجودة على موقع ويب الخاص بـ Kaspersky Lab.

صفحة التطبيق على موقع Kaspersky Lab

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

في الصفحة (<http://www.kaspersky.com/anti-virus>)، يمكنك عرض معلومات عامة حول التطبيق ووظائفه وميزاته.

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

صفحة التطبيق على موقع الدعم الفني (قاعدة المعارف)

تعتبر قاعدة المعارف عبارة عن قسم موجود على موقع الدعم الفني على الويب يقوم بتوفير النصائح المتعلقة باستخدام تطبيقات Kaspersky Lab. وتتكون قاعدة المعارف من مقالات مرجعية مصنفة حسب الموضوع.

على صفحة التطبيق في قاعدة المعارف (<http://support.kaspersky.com/kav2013>)، يمكنك قراءة مقالات تحوي معلومات وتوصيات وإجابات مفيدة عن الأسئلة الشائعة حول كيفية شراء التطبيق وتثبيته واستخدامه.

يمكن أن توفر المقالات إجابات للأسئلة التي تخرج عن نطاق Kaspersky Anti-Virus، والمتعلقة بتطبيقات Kaspersky Lab الأخرى. وقد تحتوي أيضاً على أخبار من Technical Support Service (خدمة الدعم الفني).

تعليمات عبر الإنترنت

تحتوي التعليمات عبر الإنترنت الخاصة بالتطبيق على ملفات للمساعدة.

توفر التعليمات السياقية معلومات حول كل نافذة من نوافذ التطبيق، وتسرد الإعدادات المقابلة وتصفها بالإضافة إلى قائمة المهام.

أما التعليمات الكاملة فتوفر معلومات تفصيلية حول إدارة حماية الكمبيوتر وتكوين التطبيق وحل المهام التقليدية للمستخدم.

وثائق

يوفر دليل مستخدم التطبيق معلومات حول كيفية تثبيت التطبيق وتنشيطه وتكوينه، بالإضافة إلى بيانات تشغيل التطبيق. كما تقدم الوثيقة وصفاً لواجهة التطبيق، وتوفر 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 مناقشة جديدة.

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

يتم توفير الخدمة باللغة الروسية والإنجليزية.

الاتصال بوحدة الكتابة الفنية والترجمة عن طريق البريد الإلكتروني

للاتصال بوحدة الكتابة الفنية والترجمة، أرسل رسالة بريد إلكتروني إلى docfeedback@kaspersky.com. الرجاء كتابة "Kaspersky Help Feedback: Kaspersky Anti-Virus" في سطر الموضوع الخاص برسالتك.

برنامج KASPERSKY ANTI-VIRUS

يصف هذا القسم ميزات التطبيق، كما أنه يوفر معلومات مختصرة حول وظائف التطبيق ومكوناته. ستتعرف على العناصر المضمنة في حزمة التوزيع والخدمات المتوفرة للمستخدمين المسجلين في التطبيق. ويوفر هذا القسم معلومات حول البرنامج ومتطلبات الأجهزة التي يجب أن تتوفر في الكمبيوتر للسماح للمستخدم بتنصيب التطبيق عليها.

في هذا القسم:

- 11 الجديد ما
- 11 التوزيع حزمة
- 12 وظائف الخدمة وظائف
- 13 المستخدم من خدمة
- 13 البرامج الأجهزة متطلبات

ما الجديد

يوفر Kaspersky Anti-Virus الميزات الجديدة التالية:

- لتوفير الحماية ضد الهجومات على الثغرات الأمنية للبرامج المهددة للأمان، تمت إضافة ميزة الحماية ضد البرامج المهددة للأمان إلى المكون مراقب النظام.
- تم تحسين عمل لوحة المفاتيح الظاهرية (راجع القسم "الظاهرة المفاتيح لوحة" على الصفحة 42) حيث يمكنك الآن فتحها بواسطة النقر فوق رمز بدء التشغيل السريع المعروف على حقول إدخال البيانات الموجودة على مواقع الويب.
- تم تبسيط إجراءات تثبيت التطبيق (راجع القسم "إزالة التطبيق" على الصفحة 15).
- تم تخفيض حجم قواعد البيانات المكافحة للفيروسات، مما يسمح بتقليل حجم البيانات المطلوب تنزيلها وتسريع تحديثات التثبيت.
- تم تحسين التحليل المساعد الاكتشاف المنفذ أثناء فحص مواقع الويب.

حزمة التوزيع

يمكنك شراء التطبيق بإحدى الطرق التالية:

- مغلف. موزع بواسطة المتاجر الخاصة بشركائنا.
 - من متجر الإنترنت. يتم التوزيع عبر المتاجر الإلكترونية التابعة لـ Kaspersky Lab عبر الإنترنت (مثل، <http://www.kaspersky.com>، قسم eStore) أو عبر الشركات الشريكة.
- 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 الترخيص، التي تنص على بنود وشروط استخدام التطبيق.

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

إذا قمت بشراء Kaspersky Anti-Virus من متجر عبر الإنترنت، فإنك تقوم بنسخ التطبيق من موقع الويب الخاص بالمتجر. يتم إرسال المعلومات المطلوبة لتنشيط التطبيق إليك عن طريق البريد الإلكتروني بعد السداد.

للحصول على المزيد من التفاصيل حول طرق الشراء وحزمة التوزيع، اتصل بقسم المبيعات عن طريق إرسال رسالة إلى sales@kaspersky.com.

ميزات التطبيق الأساسية

يوفر برنامج Kaspersky Anti-Virus حماية متكاملة لجهاز الكمبيوتر ضد التهديدات المعروفة والجديدة والهجوم الاحتمالي وشبكة الاتصال والبريد الإلكتروني غير المرغوب فيه والبيانات الأخرى غير المرغوب فيها. كما تتوفر وظائف مختلفة ومكونات حماية متنوعة كجزء من Kaspersky Anti-Virus 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 تكوين الإعدادات الخاصة بها.

بالإضافة إلى الحماية الثابتة التي توفرها مكونات الأمان، نوصي بأن تقوم بفحص جهاز الكمبيوتر بحثاً 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 Anti-Virus محدثاً، يجب عليك تحديث وحدات قواعد البيانات والبرامج التي يستخدمها التطبيق.

يتم تنفيذ بعض المهام التي يجب تنفيذها من حين إلى آخر (مثل إزالة تبعات أنشطة المستخدم في النظام) باستخدام الأدوات والمعالجات.

توفر مكونات الحماية التالية حراسة جهاز الكمبيوتر في الوقت الحقيقي:

فيما يلي وصف منطوق تشغيل مكونات الحماية في وضع Kaspersky Anti-Virus الموصى به من قبل المتخصصين في شركة Kaspersky Lab (أي: 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. يعترض برنامج Kaspersky Anti-Virus جميع محاولات الوصول إلى أي ملف ويفحص الملف بحثاً عن الفيروسات المعروفة. ويمكن إجراء عمليات معالجة أخرى للملف إذا لم يكن مصاباً أو إذا تمت معالجته بنجاح بواسطة التطبيق. إذا تعذر تنظيف ملف ما لأي سبب من الأسباب، فسيتم حذفه. سيتم نقل نسخته من الملف 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 خطيرة.

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.

مراقبة الشبكة

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

مكافحة الاحتيال

يمكنك مكون مكافحة الاحتيال من التحقق مما إذا كانت عناوين مواقع الويب واردة ضمن قوائم عناوين المواقع الاحتمالية. إن هذا المكون هو مكون مندمج مع مكون مكافحة فيروسات الويب، ومكون مكافحة فيروسات المراسلة الفورية.

خدمة المستخدمين

عن طريق شراء ترخيص التطبيق، يمكنك الاستفادة من الخدمات التالية أثناء فترة صلاحية الترخيص:

- تحديثات قاعدة البيانات والوصول إلى الإصدارات الجديدة من التطبيق
- الاستشارات عن طريق الهاتف والبريد الإلكتروني المتعلقة بتثبيت التطبيق وتكوينه واستخدامه
- الإخطارات الخاصة بإصدار تطبيقات جديدة بواسطة Kaspersky Lab والخاصة بالفيروسات الجديدة وانتشار الفيروسات. لتتمكن من استخدام هذه الخدمة، قم بالاشتراك في خدمة تسليم الرسائل الإخبارية عبر البريد الإلكتروني من Kaspersky Lab على موقع الدعم الفني على الويب.

لن يتم توفير أي استشارات حول الموضوعات المتعلقة بوظائف أنظمة التشغيل أو البرامج أو التكنولوجيات الخاصة بالأطراف الثالثة.

متطلبات الأجهزة والبرامج

لضمان التشغيل المناسب لبرنامج Kaspersky Anti-Virus، يجب توافق جهاز الكمبيوتر مع المتطلبات التالية:

متطلبات عامة:

- 480 ميجا بايت من المساحة الحرة على القرص الثابت (تتضمن 380 ميجا بايت على محرك النظام).
- مشغل أقراص مدمجة / أقراص DVD (لتثبيت برنامج Kaspersky لأمان الإنترنت من قرص التوزيع).
- الوصول إلى الإنترنت (لتنشيط التطبيق وتحديث قواعد البيانات والوحدات النمطية للبرنامج).
- Microsoft Internet Explorer® 8.0 أو ما يليه

• Microsoft Windows Installer 3.0.

متطلبات لـ Microsoft Windows XP Home Edition (Service Pack 2 أو أحدث)، Microsoft Windows XP Professional (Service Pack 2 أو أحدث)، و Microsoft Windows XP Professional x64 Edition (Service Pack 2 أو أحدث):

• معالج Intel® Pentium® 800 ميغا هرتز 32 بت (x86 / 64) أو ما يليه (أو مكافئ متوافق).

• ذاكرة وصول عشوائي خالية قدرها 512 ميغا بايت

متطلبات Microsoft Windows Vista® Home Basic و Microsoft Windows Vista Home Premium و Microsoft Windows Vista و Microsoft Windows Vista Business و Microsoft Windows Vista Enterprise و Microsoft Windows Vista Ultimate و Microsoft Windows 7 Starter و Microsoft Windows 7 Professional و Microsoft Windows 7 Home Premium و Microsoft Windows 7 Home Basic و Microsoft Windows 7 Ultimate:

• معالج Intel Pentium بقدرة 1 جيجا هرتز 32 بت (x86 / 64) أو أحدث (أو معالج مكافئ متوافق).

• 1 جيجا بايت من المساحة الحرة لذاكرة الوصول العشوائي (لأنظمة التشغيل 32 بت)؛ 2 جيجا بايت من المساحة الحرة لذاكرة الوصول العشوائي (لأنظمة التشغيل 64 بت).

المتطلبات الخاصة بـ Microsoft Windows 8:

• معالج Intel Pentium بقدرة 1 جيجا هرتز 32 بت (x86 / 64) أو أحدث (أو معالج مكافئ متوافق).

• 1 جيجا بايت من المساحة الحرة لذاكرة الوصول العشوائي (لأنظمة التشغيل 32 بت)؛ 2 جيجا بايت من المساحة الحرة لذاكرة الوصول العشوائي (لأنظمة التشغيل 64 بت).

تثبيت التطبيق وإزالته

يحتوي هذا القسم على إرشادات خطوة بخطوة لتثبيت التطبيق وإزالته.

في هذا القسم:

- [15](#) القياسي التثبيت إجراء
- [19](#) Kaspersky Anti-Virus من السابق الإصدار إلى تحديث
- [21](#) القياسية غير التثبيت سيدي ناربهات
- [22](#) التطبيق إزالة

إجراء التثبيت القياسي

سيتم تثبيت برنامج Kaspersky Anti-Virus على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يمكنك التنقل بينها باستخدام الزرين السابق والتالي. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر إنهاء. لإيقاف نشاط المعالج عند أي خطوة من خطوات التثبيت، قم بإغلاق نافذة المعالج.

إذا كان الهدف من التطبيق هو حماية أكثر من جهاز كمبيوتر واحد (يعتمد الحد الأقصى لعدد أجهزة الكمبيوتر على الترخيص الخاص بك)، يجب التثبيت بشكل متطابق على جميع أجهزة الكمبيوتر.

➔ تثبيت برنامج Kaspersky Anti-Virus على جهازك،

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

لتثبيت Kaspersky Anti-Virus، يمكنك أيضاً استخدام حزمة توزيع تم تنزيلها من الإنترنت. يعرض معالج الإعداد عدة خطوات إضافية للتثبيت لبعض اللغات المترجمة.

- 16... التطبيق من أحدث حزمة من عن ال بحث جاري 1. الخطوة
- 16... التطبيق تثبيت بدء 2. الخطوة
- 16... الترخيص اتفاقية مراجعة 3. الخطوة
- 17... Kaspersky أمان شبكة بيانات تجميع بيان 4. الخطوة
- 17... التطبيق تثبيت 5. الخطوة
- 18... التطبيق تثبيت إكمال 6. الخطوة
- 18... التطبيق تنشيط 7. الخطوة
- 18... المسخدم تسجيل 8. الخطوة
- 19... التفعيل استكمال 9. الخطوة

الخطوة 1. جاري البحث عن نسخة أحدث من التطبيق...

قبل الإعداد، يقوم معالج التثبيت بفحص خوادم التحديث من Kaspersky Lab بحثاً عن إصدار أحدث من برنامج Kaspersky Anti-Virus.

في حالة عدم اكتشاف معالج الإعداد لأي إصدار جديد من التطبيق على خوادم التحديث، يبدأ في تثبيت الإصدار الحالي.

في حالة اكتشاف المعالج لإصدار أحدث من Kaspersky Anti-Virus على خوادم التحديث، فإنه يعرض عليك التنزيل إلى الكمبيوتر وتثبيته. 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 رفضك لتثبيت الإصدار الجديد، يبدأ المعالج في تثبيت الإصدار الحالي من التطبيق. إذا وافقت على تثبيت الإصدار الجديد من التطبيق، يقوم معالج الإعداد بنسخ ملفات الإعداد من حزمة التوزيع إلى الكمبيوتر الخاص بك ويبدأ في تثبيت الإصدار الجديد. للحصول على المزيد من التفاصيل حول كيفية تثبيت الإصدار الجديد من التطبيق راجع المستندات ذات الصلة.

الخطوة 2. بدء تثبيت التطبيق

عند هذه الخطوة، يعرض عليك معالج الإعداد تثبيت التطبيق.

لمتابعة التثبيت، انقر زر تثبيت.

اعتماداً على نوع التثبيت ولغة الترجمة، يعرض عليك المعالج عرض اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab، بالإضافة إلى عرض مشاركتك في شبكة أمان Kaspersky.

الخطوة 3. مراجعة اتفاقية الترخيص

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Anti-Virus من حزمة التوزيع التي تم تنزيلها من الإنترنت.

عند هذه الخطوة، يعرض عليك معالج الإعداد مراجعة اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab.

قم بقراءة اتفاقية الترخيص جيداً، إذا كنت توافق على جميع الشروط الخاصة بها، انقر فوق الزر **قبول**. سوف يستمر تثبيت التطبيق.

في حالة عدم قبول اتفاقية الترخيص لن يتم تثبيت التطبيق.

الخطوة 4. بيان تجميع بيانات شبكة أمان KASPERSKY

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Anti-Virus من حزمة التوزيع التي تم تنزيلها من الإنترنت.

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، بالإضافة إلى معلومات النظام إلى Kaspersky Lab. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

استعراض بيان جمع بيانات شبكة اتصال أمان Kaspersky. إذا كنت توافق على جميع شروط الاتفاقية، حدد خانة الاختيار **أوافق على شروط المشاركة في شبكة أمان Kaspersky** في نافذة المعالج.

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

الخطوة 5. التثبيت:

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

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

يقوم Kaspersky Anti-Virus 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 الأمر.

- **توجد تطبيقات غير متوافقة على الكمبيوتر.** إذا تم اكتشاف أي تطبيقات غير متوافقة فسيتم عرضها في قائمة معروضة على الشاشة، وسيطلب منك إزالتها. تطبيقات لا يستطيع Kaspersky Anti-Virus إزالتها بشكل تلقائي، ويجب إزالتها يدوياً. أثناء إزالة التطبيقات غير المتوافقة، ستحتاج لإعادة تمهيد نظام التشغيل، بعده سيستمر تثبيت برنامج Kaspersky Anti-Virus تلقائياً.

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

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

الخطوة 6. إكمال التثبيت

عند هذه الخطوة، تخبرك نافذة المعالج هذه باكمال تثبيت التطبيق. لتشغيل برنامج Kaspersky Anti-Virus، تأكد من تحديد خانة الاختيار **تشغيل برنامج Kaspersky Anti-Virus 2013**، وانقر فوق الزر **إنهاء**.

في بعض الحالات قد تحتاج إلى إعادة تمهيد نظام التشغيل الخاص بك لإكمال التثبيت. عند تحديد خانة الاختيار **تشغيل Kaspersky Anti-Virus 2013**، سيتم تشغيل التطبيق تلقائياً بعد إعادة تمهيد نظام التشغيل.

في حالة مسح خانة الاختيار **تشغيل Kaspersky Anti-Virus 2013** قبل إغلاق المعالج، ستحتاج إلى تشغيل التطبيق يدوياً.

الخطوة 7. تنشيط التطبيق

عند هذه الخطوة، يعرض عليك معالج الإعداد تنشيط التطبيق.

يعتبر **التفعيل** عملية يتم من خلالها تفعيل الإصدار كامل الوظائف من التطبيق لفترة محددة من الوقت.

إذا قمت بشراء ترخيص لـ Kaspersky Anti-Virus وقمت بتنزيل التطبيق من متجر متوفر عبر الإنترنت، يمكن تنفيذ عملية التنشيط بشكل تلقائي أثناء التثبيت.

سُعرض عليك الخيارات التالية عند تفعيل برنامج Kaspersky Anti-Virus:

- **تفعيل الإصدار التجاري.** تحديد هذا الخيار وإدخال رمز التفعيل (انظر القسم "الترخيص حول" في صفحة 25) في حالة شراء إصدار تجاري من التطبيق.

إذا قمت بتحديد رمز تفعيل لبرنامج Kaspersky Internet Security في حقل الإدخال، فسيبدأ إجراء التحويل إلى برنامج Kaspersky Internet Security بعد الانتهاء من التفعيل.

- **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.

ستحتاج إلى الاتصال بالإنترنت لتنشيط التطبيق.

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 انقر فوق الزر **التالي** لإرسال البيانات إلى Kaspersky Lab.

في بعض الحالات يلزم تسجيل المستخدم لبدء استخدام التطبيق.

الخطوة 9. استكمال التفعيل

سيخطر ك المعالج بأن برنامج Kaspersky Anti-Virus تم تفعيله بنجاح. 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 قد قمت بطلب الاشتراك، فسيتم عرض المعلومات عن حالة الاشتراك بدلاً من تاريخ انتهاء الترخيص.

انقر الزر إنهاء لإغلاق المعالج.

تحديث إلى الإصدار السابق من KASPERSKY ANTI-VIRUS

في حالة تثبيت Kaspersky Anti-Virus 2011 أو Kaspersky Anti-Virus 2012 بالفعل على الكمبيوتر الخاص بك، يجب أن تقوم بتحديث التطبيق إلى Kaspersky Anti-Virus 2013. في حالة أن تمتلك ترخيصاً نشطاً من Kaspersky Anti-Virus 2011 أو 2012، لن يكون عليك تنشيط التطبيق: وسيقوم معالج الإعداد بشكل تلقائي باستعادة المعلومات الخاصة بترخيص Kaspersky Anti-Virus 2011 أو 2012 وتطبيقها أثناء عملية التثبيت.

سيتم تثبيت برنامج Kaspersky Anti-Virus على جهاز الكمبيوتر في وضع تفاعلي باستخدام معالج التثبيت.

يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يمكنك التنقل بينها باستخدام الزرين السابق والتالي. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر إنهاء. لإيقاف نشاط المعالج عند أي خطوة من خطوات التثبيت، قم بإغلاق نافذة المعالج.

إذا كان الهدف من التطبيق هو حماية أكثر من جهاز كمبيوتر واحد (يعتمد الحد الأقصى لعدد أجهزة الكمبيوتر على الترخيص الخاص بك)، يجب التثبيت بشكل متطابق على جميع أجهزة الكمبيوتر.

➔ تثبيت برنامج Kaspersky Anti-Virus على جهازك،

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

لتثبيت Kaspersky Anti-Virus، يمكنك أيضاً استخدام حزمة توزيع تم تنزيلها من الإنترنت. يعرض معالج الإعداد عدة خطوات إضافية للتثبيت لبعض اللغات المترجمة.

في هذا القسم:

- 20... ال تط بيق من أحدث نسخة عن ال بحث جاري 1. ال خطوة.....
- 20 ال تط بيق تثبيت بدء 2. ال خطوة.....
- 20 ال ترخيص اتفاقيات مراجعة 3. ال خطوة.....
- 20 Kaspersky أمان شبكة بيارات جميع بيات 4. ال خطوة.....
- 21 ال تثبيت 5. ال خطوة.....
- 21 ال تثبيت إكمال 6. ال خطوة.....

الخطوة 1. جاري البحث عن نسخة أحدث من التطبيق...

قبل الإعداد، يقوم معالج التنشيط بفحص خوادم التحديث من Kaspersky Lab بحثًا عن إصدار أحدث من برنامج Kaspersky Anti-Virus.

في حالة عدم اكتشاف معالج الإعداد لأي إصدار جديد من التطبيق على خوادم التحديث، يبدأ في تثبيت الإصدار الحالي.

في حالة اكتشاف المعالج لإصدار أحدث من Kaspersky Anti-Virus على خوادم التحديث، فإنه يعرض عليك التنزيل إلى الكمبيوتر وتنشيطه. يوصى بتثبيت الإصدار الحديث من التطبيق، لأن الإصدارات الأحدث تتضمن المزيد من التحسينات التي تسمح لك بضمن الحصول على حماية أفضل للكمبيوتر الخاص بك. في حالة رفضك لتثبيت الإصدار الجديد، يبدأ المعالج في تثبيت الإصدار الحالي من التطبيق. إذا وافقت على تثبيت الإصدار الجديد من التطبيق، يقوم معالج الإعداد بنسخ ملفات الإعداد من حزمة التوزيع إلى الكمبيوتر الخاص بك ويبدأ في تثبيت الإصدار الجديد. للحصول على المزيد من التفاصيل حول كيفية تثبيت الإصدار الجديد من التطبيق راجع المستندات ذات الصلة.

الخطوة 2. بدء تثبيت التطبيق

عند هذه الخطوة، يعرض عليك معالج الإعداد تثبيت التطبيق.

لمتابعة التثبيت، انقر زر **تثبيت**.

اعتمادًا على نوع التثبيت ولغة الترجمة، يعرض عليك المعالج عرض اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab، بالإضافة إلى عرض مشاركتك في شبكة أمان Kaspersky.

الخطوة 3. مراجعة اتفاقية الترخيص

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Anti-Virus من حزمة التوزيع التي تم تنزيلها من الإنترنت.

عند هذه الخطوة، يعرض عليك معالج الإعداد مراجعة اتفاقية الترخيص المبرمة بينك وبين Kaspersky Lab.

قم بقراءة اتفاقية الترخيص جيدًا، إذا كنت توافق على جميع الشروط الخاصة بها، انقر فوق الزر **قبول**. سوف يستمر تثبيت التطبيق.

في حالة عدم قبول اتفاقية الترخيص لن يتم تثبيت التطبيق.

الخطوة 4. بيان تجميع بيانات شبكة أمان KASPERSKY

يتم عرض هذه الخطوة من المعالج لبعض لغات الترجمة عند تثبيت Kaspersky Anti-Virus من حزمة التوزيع التي تم تنزيلها من الإنترنت.

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، بالإضافة إلى معلومات النظام إلى Kaspersky Lab. لا يتم تجميع أو معالجة أو تخزين أي بيانات خاصة مستلمة.

استعراض بيان جمع بيانات شبكة اتصال أمان Kaspersky. إذا كنت توافق على جميع شروط الاتفاقية، حدد خانة الاختيار **أوافق على شروط المشاركة في شبكة أمان Kaspersky** في نافذة المعالج.

انقر فوق الزر **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 Anti-Virus 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 الأمر.

- **توجد تطبيقات غير متوافقة على الكمبيوتر.** إذا تم اكتشاف أي تطبيقات غير متوافقة فسيتم عرضها في قائمة معروضة على الشاشة، وسيطلب منك إزالتها. تطبيقات لا يستطيع Kaspersky Anti-Virus إزالتها بشكل تلقائي، ويجب إزالتها يدويًا. أثناء إزالة التطبيقات غير المتوافقة، ستحتاج لإعادة تمهيد نظام التشغيل، بعده سيستمر تثبيت برنامج Kaspersky Anti-Virus 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 باكمال تثبيت التطبيق بنجاح.

أعد تشغيل نظام التشغيل بعد أن يتم تثبيت التطبيق.

عند تحديد خانة الاختيار **تشغيل Kaspersky Anti-Virus 2013** ، سيتم تشغيل التطبيق تلقائيًا بعد إعادة تمهيد نظام التشغيل.

في حالة مسح خانة الاختيار **تشغيل Kaspersky Anti-Virus** قبل إغلاق المعالج، ستحتاج إلى تشغيل التطبيق يدويًا.

سيناريوهات التثبيت غير القياسية

يصف هذا القسم سيناريوهات تثبيت التطبيق التي تختلف عن السيناريوهات الخاصة بالتثبيت القياسي أو التحديث من الإصدار السابق.

تثبيت Kaspersky Anti-Virus وتنشيطه باستخدام رمز التنشيط الخاص بـ Kaspersky Internet Security

إذا قمت، خلال تثبيت Kaspersky Anti-Virus، واثنا خطوة تنشيط التطبيق بإدخال رمز تنشيط خاص ببرنامج Kaspersky Internet Security، سيبدأ تشغيل معالج الإعداد، والذي ينتج عنه تثبيت Kaspersky Internet Security على الكمبيوتر الخاص بك.

في حالة أنك قمت، أثناء تثبيت Kaspersky Anti-Virus، وعند خطوة تنشيط التطبيق، بتحديد **التفعيل لاحقاً** ثم قمت بتنشيط التطبيق المثبت باستخدام رمز تنشيط خاص ببرنامج Kaspersky Internet Security، سيتم أيضاً بدء تشغيل معالج الترحيل، والذي ينتج عنه التحويل تحويل Kaspersky Anti-Virus إلى Kaspersky Internet Security.

تثبيت Kaspersky Anti-Virus 2013 فوق Kaspersky Internet Security 2011 أو Kaspersky Internet Security 2012

إذا قمت بتشغيل تثبيت Kaspersky Anti-Virus 2013 على كمبيوتر تم بالفعل تثبيت Kaspersky Internet Security 2011 أو Kaspersky Internet Security 2012 له ترخيص نشط عليه، سيقوم معالج الإعداد باكتشاف هذا الأمر ومطالبتك بتحديد أي من الخيارات التالية:

- الاستمرار في استخدام Kaspersky Internet Security في ظل الترخيص الحالي. في هذه الحالة، سيبدأ تشغيل معالج الترحيل، والذي ينتج عنه تثبيت Kaspersky Internet Security 2013 على الكمبيوتر الخاص بك. سيكون بإمكانك استخدام Kaspersky Internet Security 2013 طالما أن ترخيص Kaspersky Internet Security 2011 أو Kaspersky Internet Security 2012 لا يزال سارياً.
- متابعة تثبيت Kaspersky Anti-Virus 2013. في هذه الحالة، سيستمر إجراء التثبيت حسب السيناريو القياسي، مع البدء بخطوة تفعيل التطبيق.

إزالة التطبيق

بعد إلغاء تثبيت برنامج Kaspersky لأمان الإنترنت، سيصبح جهاز الكمبيوتر والبيانات الشخصية غير محميين.

يتم إلغاء تثبيت برنامج Kaspersky Anti-Virus بمساعدة معالج الإعداد.

➔ لبدء تشغيل المعالج،

في القائمة ابدأ، حدد البرامج □ Kaspersky Anti-Virus 2013 □ إزالة Kaspersky Anti-Virus 2013.

في هذا القسم:

- [22](#) الاستمرار في استخدام إعادة الإصدار 1. الخطوة
- [23](#) التطبيق في إزالة تأكيد 2. الخطوة
- [23](#) الإزالة استكمال التطبيق في إزالة 3. الخطوة

الخطوة 1. حفظ البيانات لإعادة الاستخدام

عند هذه الخطوة، يمكنك تحديد أي من البيانات التي يستخدمها التطبيق تريد أن تحتفظ بها للاستخدام المتكرر أثناء التثبيت التالي للتطبيق (على سبيل المثال، إصدار أحدث من التطبيق).

بشكل افتراضي، يطالبك التطبيق بحفظ المعلومات الخاصة بالتنشيط.

➔ لحفظ البيانات من أجل استخدامها لاحقاً، حدد خانة الاختيار الموجودة بجوار عناصر البيانات التي تريد حفظها:

- **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.
- **ملفات العزل** – الملفات التي تم فحصها بواسطة التطبيق وتم نقلها إلى العزل.

بعد أن تتم إزالة Kaspersky Anti-Virus من الكمبيوتر، تصبح الملفات المعزولة غير متوفرة. يجب أن تقوم بتثبيت Kaspersky Anti-Virus لتتمكن من معالجة هذه الملفات.

- تعتبر إعدادات تشغيل التطبيق هي قيم إعدادات التطبيق المحددة أثناء التكوين.

لا يضمن Kaspersky Lab دعم الإعدادات من الإصدار السابق للتطبيق. بعد تثبيت إصدار أحدث من التطبيق، نوصيك بفحصه للتحقق من صحة تكوينه.

- بيانات iChecker هي ملفات تحتوي على معلومات حول الكائنات التي تم فحصها بالفعل باستخدام تقنية iChecker.

الخطوة 2. تأكيد إزالة التطبيق

لأن إزالة التطبيق يهدد أمان جهاز الكمبيوتر والبيانات الشخصية، سيطلب منك التأكيد على رغبتك في إزالة التطبيق. للقيام بذلك، انقر الزر إزالة.

الخطوة 3. إزالة التطبيق. استكمال الإزالة

في هذه الخطوة، يقوم المعالج بإزالة التطبيق من جهاز الكمبيوتر. الرجاء الانتظار حتى اكتمال 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

يتضمن هذا القسم معلومات حول المفاهيم الأساسية لتنشيط التطبيق. قم بقراءة هذا القسم لتتعرف على المزيد حول الهدف من اتفاقية الترخيص وأنواع التراخيص وطرق تنشيط التطبيق وتجديد الترخيص.

في هذا القسم:

- 24 إل نهائي المستخدم ترخيص اتفاقية حول
- 24 إل ترخيص حول
- 25 إل تنشيط رمز حول
- 25 إل بيانات تزويد حول

حول اتفاقية ترخيص المستخدم النهائي

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

قم بقراءة البنود والشروط الخاصة باتفاقية الترخيص بعناية قبل أن تقوم ببدء استخدام التطبيق.

تُعتبر موافقاً على بنود اتفاقية الترخيص بعد تأكيد موافقتك على اتفاقية الترخيص عند تثبيت التطبيق. إذا لم تقبل شروط اتفاقية الترخيص، يجب إحباط تثبيت التطبيق أو التخلي عن استخدام التطبيق.

حول الترخيص

يعتبر الترخيص عبارة عن حق محدد بوقت لاستخدام التطبيق، ويتم منحه بموجب اتفاقية ترخيص المستخدم النهائي. يحتوي الترخيص على رمز فريد لتنشيط نسختك من Kaspersky Anti-Virus.

يمكنك أي ترخيص ساري 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 "المستخدمين خدمات" على الصفحة 13).

يعتمد نطاق فترة استخدام الخدمات والتطبيقات على نوع الترخيص الذي تم تنشيط التطبيق أسفله.

يتم توفير أنواع الترخيص التالية:

- تجريبي – ترخيص مجاني يهدف إلى تجربة التطبيق.

عادة تكون صلاحية الترخيص المجاني عبارة عن مدة قصيرة. وبمجرد انتهاء مدة الترخيص التجريبي، يتم تعطيل جميع ميزات Kaspersky Anti-Virus. لمتابعة استخدام التطبيق، تحتاج إلى شراء ترخيص تجاري.

- تجاري – ترخيص مدفوع يتم تقديمه عند شراء التطبيق.

عندما تنتهي الرخصة التجارية، فإن التطبيق يظل قيد التشغيل ولكن بوظائف محدودة (على سبيل المثال، التحديث واستخدام شبكة اتصال أمان Kaspersky تكون غير متوفرة). لا يزال بإمكانك الاستفادة من مكونات التطبيق وتنفيذ عمليات الفحص للبحث عن الفيروسات والبرامج الضارة الأخرى، ولكن باستخدام قواعد البيانات التي تم تثبيتها قبل انتهاء صلاحية الترخيص فقط. لمتابعة استخدام Kaspersky Anti-Virus 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 رمز التنشيط

يعتبر رمز التنشيط عبارة عن رمز تستلمه عند شراء الترخيص التجاري لـ Kaspersky Anti-Virus. 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:

- إذا قمت بشراء الإصدار المعلن من برنامج Kaspersky Anti-Virus، يتم تحديد رمز التنشيط في الوثائق أو على العبوة التي تحتوي على القرص المضغوط للإعداد.
- إذا قمت بشراء برنامج Kaspersky Anti-Virus من أحد المتاجر المنتشرة عبر الإنترنت، يتم إرسال رمز التنشيط إلى عنوان البريد الإلكتروني الذي قمت بتحديدته عند طلب المنتج.

يبدأ العد التنازلي لفترة الترخيص من تاريخ تنشيط التطبيق. إذا قمت بشراء ترخيص يستهدف لاستخدام Kaspersky Anti-Virus على أجهزة متعددة، يبدأ العد التنازلي لمدة الترخيص من لحظة تطبيق رمز التنشيط.

إذا فقدت أن قمت بشكل عرضي بحذف رمز التنشيط بعد التنشيط، يجب أن ترسل طلبًا إلى خدمة الدعم الفني في Kaspersky Lab من حسابي في Kaspersky (راجع القسم "Kaspersky في حسابي من الدعم الفني" على الصفحة 60).

حول تزويد البيانات

لزيادة مستوى الحماية عن طريق قبول أحكام اتفاقية الترخيص، فإنك توافق على توفير المعلومات التالية إلى Kaspersky Lab في الوضع التلقائي:

- معلومات حول مجموعات الملفات المعالجة (MD5)؛
- المعلومات المطلوبة لتقييم سمعة عناوين URL؛
- إحصائيات استخدام إخطارات المنتج؛
- البيانات الإحصائية حول الحماية ضد البريد الإلكتروني غير المرغوب فيه؛
- بيانات حول تنشيط Kaspersky Anti-Virus والإصدار المستخدم حاليًا؛
- معلومات حول أنواع التهديدات المكتشفة؛

- معلومات حول الشهادات الرقمية المستخدمة حاليًا والمعلومات المطلوبة للتحقق من صحتها.

إذا كان الكمبيوتر مزودًا بـ TPM (الوحدة النمطية للنظام الأساسي الموثوق به)، فإنك توافق أيضًا على تزويد Kaspersky Lab بتقرير TPM حول تمهيد نظام التشغيل وتوفير المعلومات المطلوبة للتحقق منه. في حالة حدوث خطأ أثناء تثبيت Kaspersky Anti-Virus، فإنك توافق على توفير معلومات لـ Kaspersky Lab حول رمز الخطأ، وحزمة التوزيع المستخدمة حاليًا، والكمبيوتر الخاص بك في الوضع التلقائي.

في حالة المشاركة في Kaspersky Security Network (KSN) (راجع القسم "Kaspersky Security Network في ال مشاركة" على الصفحة 56)، يتم إرسال المعلومات التالية بشكل تلقائي من الكمبيوتر إلى Kaspersky Lab:

- معلومات حول الأجهزة والبرامج المثبتة على الكمبيوتر؛
- معلومات حول حالة الحماية المكافحة للفيروسات للكمبيوتر، بالإضافة إلى جميع الكائنات والإجراءات المحتمل كونها خبيثة والقرارات المتخذة فيما يتعلق بهذه الكائنات والإجراءات؛
- معلومات حول التطبيقات الجاري تنزيلها وتشغيلها؛
- معلومات حول أخطاء الواجهة واستخدام واجهة Kaspersky Anti-Virus؛
- معلومات حول إصدار قواعد البيانات المكافحة للفيروسات المستخدمة حاليًا؛
- إحصائيات التحديثات والاتصالات بخوادم Kaspersky Lab؛
- إحصائيات الفترات الزمنية الفعلية التي تقضيها مكونات التطبيق لفحص الأجسام.

كذلك، فقد تتطلب عمليات الفحص الإضافية التي تتم في Kaspersky Lab إرسال الملفات (أو أجزاء منها) التي تمثل خطرًا متزايدًا لتمكين المهاجمين من إلحاق الضرر بالكمبيوتر أو البيانات الخاصة بالمستخدم.

تتم حماية المعلومات المستردة بواسطة Kaspersky Lab حسب المتطلبات المنصوص عليها بواسطة التشريعات الموجودة. تستخدم Kaspersky Lab أي معلومات مستردة كإحصائيات عامة فقط. يتم توفير الإحصائيات العامة تلقائيًا باستخدام معلومات أصلية مستردة، وهي لا تتضمن أي بيانات خاصة أو معلومات سرية أخرى. يتم تخزين المعلومات الأصلية المستردة في صيغة مشفرة؛ ويتم مسحها عند جمعها (مرتين سنويًا). يتم تخزين الإحصائيات العامة بشكل غير محدود.

حل المهام النمطية

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

- 29 التثبيت وتنشيط
- 30 وتغييره الترخيص على الحصول
- 30 التثبيت وإخطارات إدارة
- 31 الأمان موضوعات وحل الكمبيوتر حماية حالة تقييم
- 32 التثبيت ووحدات البيانات وإعادة تحديث
- 32 الفيروسات عن البحث بك الخاص الكمبيوتر في الحرجة المناطق فحص
- 32 الفيروسات عن البحث لكمبيوتر كامل فحص
- 33 الفيروسات عن بحثًا آخر كائن أي أو قرص أو مجلد أو ملف فحص
- 34 إزالة الصامتة الكائنات فحص
- 35 التثبيت بواسطة نظيفه أو حذفه تم كائن استعادة
- 36 الإصابتة بعد التشغيل نظام استعادة
- 38 الإلكتروليت البريد رسائل مرفقات وصفية الإلكتروليت البريد فحص
- 39 الأمانة الثغرات عن بحثًا الكمبيوتر فحص
- 39 تثبيت إيقال سمعة فحص
- 40 السرقة ضد الشخصية البيانات حماية
- 46 الويب لموقع الأمانة الحالة تقييم
- 47 الشاشة ملء ووضع الألعاب تعرف ملف استخدام
- 47 واستخدامه الإنقاذ قرص إنشاء
- 50 المرور كامة مراسد تخدا Kaspersky Anti-Virus برنامج إلى الوصول تقييم
- 51 واستعادتها الكمبيوتر حماية إيقاف
- 51 التثبيت وتنشيط تقرير عرض
- 52 الأفضلية التثبيت إعدادات استعادة
- 54 آخر كمبيوتر على الأمانة تثبيت Kaspersky Anti-Virus إلى التثبيت إعدادات استيراد
- 54 الذاكرة Kaspersky أدوات استخدام
- 56 Kaspersky (KSN) أمان شبكة في المشاركة

57 Kaspersky Internet Security برنامج إلى Kaspersky Anti-Virus برنامج من الـ تحديث كـيفية

تنشيط التطبيق

يجب أن تقوم بتنشيط التطبيق لتتمكن من استخدام الوظائف والخدمات المقترنة بها.

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

➔ لتشغيل معالج تنشيط برنامج Kaspersky Anti-Virus، قم بتنفيذ أحد الإجراءات التالية:

- انقر فوق الارتباط **تنشيط** في نافذة إشعار Kaspersky Anti-Virus التي تظهر في منطقة إخطارات شريط المهام.
- انقر فوق الارتباط **أدخل رمز التنشيط** الموجود في الجزء السفلي من نافذة التطبيق الرئيسية. في النافذة **التراخيص** التي ستفتح، انقر فوق الزر **تنشيط التطبيق**.

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

1.Step. أدخل رمز التنشيط

أدخل رمز التنشيط (راجع القسم "التنشيط رمز حول" على الصفحة 25) في الحقل المقابل وانقر فوق الزر **التالي**.

2.Step. طلب التنشيط

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

3.Step. إدخال بيانات التسجيل

يُسمح للمستخدمين المسجلين استخدام الميزات التالية:

- إرسال طلبات إلى خدمة الدعم الفني ومعمل مكافحة الفيروسات من حساب Kaspersky الخاص بي على موقع الويب لـ Kaspersky Lab
- إدارة رموز التنشيط؛
- استلام المعلومات حول المنتجات الجديدة والعروض الخاصة من Kaspersky Lab.

حدد بيانات التسجيل الخاصة بك وانقر الزر **التالي**.

4.Step. التفعيل

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

5.Step. اكتمال المعالج

تعرض نافذة هذا المعالج معلومات عن نتائج الأنشطة.

انقر الزر **إنهاء** لإغلاق المعالج.

الحصول على الترخيص وتجديده

إذا قمت بتنصيب برنامج Kaspersky Anti-Virus بدون ترخيص، يمكنك شراء ترخيصًا بعد التنصيب. عند الحصول على ترخيص ستلقى رمزًا للتنصيب يجب عليك تطبيقه من أجل تفعيل التطبيق (راجع القسم "التطبيق تفعيل" على الصفحة 29).

وعندما ينتهي ترخيصك، يمكنك تجديده. لتنفيذ هذا الأمر، يمكنك إضافة رمز تنشيط دون الانتظار حتى موعد انتهاء صلاحية الترخيص الحالي. عند انتهاء صلاحية الترخيص الحالي، سيقوم Kaspersky Anti-Virus بالتنشيط التلقائي باستخدام رمز التنشيط الإضافي.

➔ لشراء ترخيص:

1. افتح نافذة التطبيق الرئيسية.
 2. انقر فوق الارتباط **أدخل رمز التنشيط هنا / الترخيص** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة الترخيص.
 3. في النافذة التي ستفتح، انقر فوق الزر **شراء رمز التنشيط**.
- سيتم فتح صفحة ويب eStore التي يمكنك من خلالها شراء الترخيص.

➔ لإضافة رمز تنشيط احتياطي:

1. افتح نافذة التطبيق الرئيسية.
 2. انقر فوق الارتباط **أدخل رمز التنشيط هنا / الترخيص** في الجزء الأسفل من النافذة الرئيسية ليتم فتح النافذة الترخيص.
 3. في النافذة التي ستفتح، انقر فوق الزر **أدخل رمز التنشيط**.
- ستم فتح "معالج تنشيط التطبيق".
4. أدخل رمز التنشيط في الحقول المقابلة وانقر فوق الزر **التالي**.
- سيقوم Kaspersky Anti-Virus بإرسال البيانات إلى خادم التنشيط للتحقق من صحتها. في حالة نجاح التحقق من الصحة، سيتابع معالج التنشيط تلقائيًا إلى الخطوة التالية.
5. عند الانتهاء من المعالج، انقر فوق الزر **إنهاء**.

إدارة إخطارات التطبيق

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

- **إخطارات حرجة** – تخبرك هذه الإخطارات بالأحداث التي لها أهمية حرجة لأمان الكمبيوتر، مثل اكتشاف وجود كائن خبيث أو نشاط خطير في النظام. نوافذ الإخطارات الحرجة والرسائل المنبثقة حمراء اللون.
- **إخطارات هامة** - تخبرك بالأحداث ذات الأهمية المحتملة لأمان الكمبيوتر، مثل اكتشاف الكائن محتمل الإصابة أو النشاط المريب في النظام. نوافذ الإخطارات الهامة والرسائل المنبثقة صفراء اللون.
- **إخطارات معلوماتية** – تخبرك بالأحداث التي ليس لها أهمية حرجة لأمان الكمبيوتر. نوافذ الإخطارات المعلوماتية والرسائل المنبثقة خضراء اللون.

في حالة عرض إخطار على الشاشة، يجب تحديد أحد الخيارات المقدمة. ويعتبر الخيار الأمثل هو الخيار الموصى به كالخيار الافتراضي من خلال خبراء Kaspersky Lab experts.

تقييم حالة حماية الكمبيوتر وحل موضوعات الأمان

تظهر مشكلات حماية جهاز الكمبيوتر من خلال المؤشر الموجود في الجزء الأيمن من النافذة الرئيسية للتطبيق. يظهر المؤشر على شكل رمز على الشاشة يتغير لونه اعتمادًا على حالة حماية الكمبيوتر: الأخضر يعني أن الكمبيوتر محمي، والأصفر يشير إلى وجود مشكلات تتعلق بالحماية أما الأحمر فيعتبر تنبهاً لوجود تهديدات خطيرة لأمان الكمبيوتر. ويوصى بالمعالجة الفورية للتغلب على المشكلات وتهديدات الأمان.



الشكل 1. نافذة حالة الحماية

بالنقر فوق المؤشر في نافذة التطبيق الرئيسية، سيتم فتح النافذة مشكلات الأمان (انظر الشكل أدناه) التي تحتوي على معلومات مفصلة حول حالة حماية جهاز الكمبيوتر واقتراحات إصلاح المشكلات والتهديدات المكتشفة.



الشكل 2. نافذة مشكلات الأمان

يتم تجميع المشكلات المتعلقة بالحماية حسب الفئات. لكل مشكلة، يتم سرد الإجراءات التي يمكن استخدامها لحل المشكلة.

تحديث قواعد البيانات و وحدات التطبيق

يقوم برنامج Kaspersky Anti-Virus بشكل افتراضي بالبحث تلقائياً عن التحديثات على خوادم Kaspersky Lab. في حالة قيام الخادم بتخزين مجموعة من التحديثات الحديثة، سيقوم Kaspersky Anti-Virus بتنزيل التحديثات وتثبيتها في وضع الخلفية. يمكنك تشغيل تحديث Kaspersky Anti-Virus يدوياً في أي وقت من نافذة التطبيق الرئيسية أو من قائمة سياق رمز التطبيق الموجود في منطقة إخطارات شريط المهام.

لتحميل تحديثات من خوادم Kaspersky Lab، ينبغي أن تكون متصلاً بالإنترنت.

➔ 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 وحدد القسم تحديث في الجزء الأيمن من النافذة.

2. في النافذة تحديث التي ستفتح، انقر الزر تشغيل التحديث.

فحص المناطق الحرجة في الكمبيوتر الخاص بك للبحث عن الفيروسات

يتضمن فحص المناطق الحرجة فحص الكائنات التالية:

- الكائنات المحملة عند بدء تشغيل نظام التشغيل؛
- ذاكرة النظام؛
- أقسام التمهيد للقرص.

➔ لبدء تشغيل الفحص الكامل من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية وحدد القسم فحص في الجزء الأيمن من النافذة.



2. في النافذة الفحص التي سيتم فتحها، في القسم فحص المناطق الحرجة، انقر فوق الزر

فحص كامل للكمبيوتر للبحث عن الفيروسات

أثناء الفحص الكامل، يقوم Kaspersky Anti-Virus بفحص الكائنات التالية بشكل افتراضي:

- ذاكرة النظام؛
- الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل؛
- النسخ الاحتياطي للنظام؛

- المحركات الثابتة والمحركات القابلة للإزالة.

نوصي بتشغيل فحص كامل بشكل فوري بعد تثبيت Kaspersky Anti-Virus على الكمبيوتر.

▶ لبدء تشغيل الفحص الكامل من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية وحدد القسم **فحص** في الجزء الأيمن من النافذة.



2. في النافذة **الفحص** التي سيتم فتحها، في القسم **فحص كامل**، انقر فوق الزر

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 نافذة التطبيق الرئيسية،
- استخدام Kaspersky Anti-Virus Gadget (راجع القسم "Kaspersky Gadget | استخدام" على الصفحة 54) (فقط لنظامي التشغيل Microsoft Windows Vista و Microsoft Windows 7).

▶ 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 الخاصة بكائن في Microsoft Windows

➔ لبدء فحص كائن من نافذة التطبيق الرئيسية:

1. افتح نافذة التطبيق الرئيسية وحدد القسم **فحص** في الجزء الأيمن من النافذة.
 2. انقر فوق الارتباط **استعراض** في الجزء الأيسر السفلي من النافذة لفتح النافذة **فحص مخصص**، وحدد خانة الاختيار التي بجوار المجلدات والأقراص التي تحتاج إلى فحصها.
- في حالة عدم عرض النافذة لأي كائن مطلوب فحصه:

a. انقر فوق الزر **إضافة**

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

➔ لفحص كائن للبحث عن الفيروسات باستخدام الأداة

اسحب الكائن المطلوب فحصه على الأداة.

فحص الكائنات محتملة الإصابة

في حالة الاشتباه في إصابة كائن ما، فقم أولاً بفحصه باستخدام برنامج Kaspersky Anti-Virus (راجع القسم "فحص كيفية" في دليل الفيروسات عن بحثًا آخر كائن أو قرص أو مجلد أو ملف" في صفحة 33).

إذا قام التطبيق بإكمال الفحص وحدد أن الكائن آمن على الرغم من أنك كنت تشك فيه، يمكنك إرسال هذا الكائن إلى Anti-Virus Lab: يقوم خبراء معمل الفيروسات بفحص الكائن. وإذا اكتشف أنه مصاب بفيروس، فإنهم يقومون على الفور بإضافة وصف

الفيروس الجديد إلى قواعد البيانات التي سيقوم التطبيق بتنزيلها مع تحديث (انظر القسم " بيانات قواعد تحديث كيفة التطبيق " في صفحة 32).

➔ لإرسال ملف إلى معمل الفيروسات:

1. انتقل إلى صفحة الطلب الخاصة بمعمل الفيروسات (<http://support.kaspersky.com/virlab/helpdesk.html>).

2. اتبع التعليمات الواردة في هذه الصفحة لإرسال الطلب الخاص بك.

استعادة كائن تم حذفه أو تنظيفه بواسطة التطبيق

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

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

لا يقوم برنامج Kaspersky Anti-Virus بتنظيف تطبيقات نمط Metro. إذا اكتشفت إحدى عمليات الفحص خطوة أحد التطبيقات، فستتم إزالته من الكمبيوتر.

عند حذف كائنات لتطبيقات على نمط Metro، لن يقوم Kaspersky Anti-Virus بإنشاء أي نسخ احتياطية. لاستعادة هذه الكائنات، يجب استخدام أدوات الاستعادة الخاصة بنظام التشغيل الخاص بك (للحصول على التفاصيل، راجع الوثائق الملحق بنظام التشغيل المثبت على الكمبيوتر الخاص بك) أو قم بتحديث التطبيقات عبر متجر Windows.

➔ لاستعادة ملف تم حذفه أو تنظيفه بواسطة التطبيق:

1. افتح نافذة التطبيق الرئيسية.

2. في الجزء الأسفل من النافذة، حدد القسم العزل.

3. في النافذة العزل التي سيتم فتحها، حدد الملف المطلوب من القائمة وانقر فوق الزر استعادة (راجع الشكل الموجود أدناه).



الشكل 4. نافذة العزل

استعادة نظام التشغيل بعد الإصابة

إذا كنت تشك في أن نظام التشغيل الخاص بالكمبيوتر الخاص بك تالفاً أو تم تعديله بسبب نشاط برنامج ضار أو بسبب فشل النظام، استخدم معالج استكشاف مشكلات Microsoft Windows وإصلاحها ما بعد الإصابة والتي تقوم بإزالة أي تتبعات للكائنات الخبيثة من على النظام. 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 مختلفة لهذه الأنواع من الأضرار. وقد تتضمن هذه الأسباب نشاط برامج خبيثة أو تكوين النظام بشكل خاطئ أو فشل 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 اللازمة لتنفيذها للتخلص من المشكلات. ويقوم المعالج بتصنيف هذه الإجراءات إلى فئات بناءً على درجة خطورة المشكلات المكتشفة.

➔ لبدء تشغيل معالج استكشاف أخطاء Microsoft Windows وإصلاحها لما بعد الإصابة:

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء الأسفل من النافذة، حدد القسم الأدوات.
3. في النافذة التي سيتم فتحها، في القسم استكشاف أخطاء Microsoft Windows وإصلاحها، انقر فوق الزر بدء.

سيتم فتح النافذة معالج استكشاف أخطاء Microsoft Windows وإصلاحها لما بعد الإصابة.

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

دعنا نفحص خطوات المعالج بالتفصيل.

1Step. بدء استعادة النظام

تأكد من تحديد خيار المعالج للبحث عن المشكلات الناتجة عن نشاط البرمجيات الخبيثة وانقر الزر التالي.

2Step. البحث عن المشكلات

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

3Step. 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. وينصح بتنفيذ جميع الإجراءات في هذه المجموعة.
- إجراءات مستحسنة وهي الإجراءات التي تساعد على القضاء على المشكلات التي تمثل تهديداً محتملاً. وينصح كذلك بتنفيذ جميع الإجراءات في هذه المجموعة.
- 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 المتوافق. وافترضياً، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا لم ترغب في تنفيذ إجراء معين، قم بإلغاء تحديد المربع المجاور له.

يوصى بشدة عدم إلغاء تحديد خانة الاختيار المحددة افتراضياً لأن القيام بذلك سوف يجعل الكمبيوتر عرضة للتهديدات.

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر الزر التالي.

4Step. إصلاح المشكلات

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

5Step. اكتمال المعالج

انقر الزر إنهاء لإغلاق المعالج.

فحص البريد الإلكتروني وتصفية مرفقات رسائل البريد الإلكتروني

يسمح لك Kaspersky Anti-Virus بفحص رسائل البريد الإلكتروني للبحث عن الكائنات الخطيرة باستخدام مكون مكافحة فيروسات البريد. يبدأ تشغيل مكون مكافحة فيروسات البريد عندما يتم تشغيل نظام التشغيل ويظل في ذاكرة الوصول العشوائي بشكل دائم، ويقوم بفحص جميع رسائل البريد الإلكتروني التي يتم إرسالها أو استلامها من خلال بروتوكولات POP3 و SMTP و IMAP و MAPI و NNTP، بالإضافة إلى الاتصالات المشفرة (SSL) من خلال POP3 و SMTP و IMAP.

وبشكل افتراضي، يفحص مكون مكافحة فيروسات البريد كلا من الرسائل الواردة والصادرة. عند الضرورة، يمكنك تمكين فحص الرسائل الواردة فقط.

➔ لفحص رسائل البريد الإلكتروني الواردة 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.
- سيتم فتح النافذة مكافحة فيروسات البريد.
5. في النافذة التي ستفتح، استخدم علامة التبويب عام في القسم نطاق الحماية لتحديد الخيار الرسائل الواردة فقط.

في حالة عدم اكتشاف تهديدات في رسالة البريد الإلكتروني، أو في حالة تنظيف جميع الكائنات المصابة بنجاح، ستصبح الرسالة متوفرة للعمليات التالية. في حالة فشل المكون في تنظيف الكائن المصاب، يقوم مكون مكافحة فيروسات البريد بإعادة تسمية الكائن من الرسالة وتوسيع موضوع الرسالة مع وجود إخطار يفيد بمعالجة الرسالة بواسطة Kaspersky Anti-Virus. قبل حذف أحد الكائنات، يقوم Kaspersky Anti-Virus بإنشاء نسخة احتياطية منه ووضع هذه النسخة في العزل (راجع القسم "كائنات استعادة التثبيت بواسطة ماص أو محذوف" على الصفحة 35).

يمكن أن تنتشر البرامج الخبيثة على شكل مرفقات في رسائل البريد الإلكتروني. يمكنك تمكين تصفية المرفقات في رسائل البريد الإلكتروني. تسمح التصفية بإعادة التسمية التلقائية أو حذف الملفات المرفقة التابعة للأنواع المحددة.

➔ 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.
- سيتم فتح النافذة مكافحة فيروسات البريد.

5. في النافذة التي ستفتح، على علامة التبويب **عامل تصفية المرفقات** حدد وضع تصفية المرفقات (إعادة تسمية أنواع المرفقات المحددة أو حذف أنواع المرفقات المحددة).
6. من قائمة أنواع الملفات (الملحقات) حدد أنواع المرفقات التي يجب تصفيتها.
إذا كنت ترغب في إضافة قناع لنوع الملف الجديد:
a. انقر فوق الارتباط **إضافة** في الجزء السفلي من النافذة ليتم فتح النافذة **إدخال قناع لاسم الملف**.
b. في النافذة التي سيتم فتحها، اكتب قناع نوع الملف.
7. انقر فوق الزر **تطبيق** في النافذة **الإعدادات**.

فحص الكمبيوتر بحثاً 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 وحدد القسم **فحص** في الجزء الأيمن من النافذة.



2. في النافذة **الفحص** التي سيتم فتحها، في القسم **فحص الثغرات الأمنية**، انقر فوق الزر

فحص سمعة التطبيق

يسمح لك Kaspersky Anti-Virus بمعرفة سمعة التطبيقات من المستخدمين المتواجدين في جميع أنحاء العالم. وتتضمن سمعة التطبيق المعايير التالية:

- اسم المورد؛
- معلومات حول التوقيع الرقمي (متوفر في حالة وجود توقيع رقمي)؛
- معلومات حول المجموعة التي تم تعيين التطبيق إليها بواسطة معظم مستخدمي شبكة أمان Kaspersky؛
- عدد مستخدمي شبكة أمان Kaspersky الذين يستخدمون التطبيق (متوفر في حالة تضمين التطبيق في مجموعة الثقة في قاعدة بيانات شبكة أمان Kaspersky)؛
- الوقت الذي يُصبح فيه التطبيق معروفًا في شبكة أمان Kaspersky؛
- الدول التي ينتشر بها التطبيق

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

افتح قائمة سياق الملف التنفيذي للتطبيق وحدد فحص السمعة في KSN (راجع الشكل الموجود أدناه).



الشكل 5. قائمة السياق الخاصة بكانن في Microsoft Windows

سيتم فتح نافذة تتضمن معلومات حول سمعة التطبيق في KSN

انظر أيضًا:

56 Kaspersky (KSN) أمان شبكة في المشاركة

حماية البيانات الشخصية ضد السرقة

يساعدك برنامج Kaspersky Anti-Virus على حماية بياناتك الخاصة ضد السرقة:

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

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

يتم ضمان الحماية ضد الاحتيال بواسطة مكافحة الاحتيال التي تنفذ في مكونات مكافحة فيروسات الويب ومكافحة فيروسات المراسلة الفورية.

تضمن الحماية ضد اعتراض البيانات المدخلة باستخدام لوحة المفاتيح عن طريق استخدام لوحة المفاتيح الظاهرية ومدير كلمات المرور.

تم تصميم معالج منظف الخصوصية لإزالة جميع المعلومات الخاصة بأنشطة المستخدم من على الكمبيوتر.

في هذا القسم:

- 41..... الاحتيال ضد الحماية
- 42..... الظاهرة المفاتيح لوحة
- 43..... الخصوصية من نظف

الحماية ضد الاحتيال

يتم ضمان الحماية ضد الاحتيال بواسطة مكافحة الاحتيال التي تنفذ في مكونات مكافحة فيروسات الويب ومكافحة 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 مركز الحماية وحدد القسم الفرعي مكافحة فيروسات الويب وانقر فوق الزر إعدادات.
- سيتم فتح النافذة مكافحة فيروسات الويب.
4. في النافذة التي سيتم فتحها، من علامة التبويب عام، في القسم مستشار Kaspersky لعناوين URL وحدد خانة الاختيار التحقق من صفحات الويب بحثاً عن الاحتيال.
 5. إذا كنت ترغب في أن يستخدم مكون مكافحة الاحتيال التحليل المساعد على الاكتشاف، انقر فوق الزر إضافي عند فحص صفحات الويب.
- سيتم فتح النافذة إعدادات مكافحة الاحتيال.
6. في النافذة التي سيتم فتحها، حدد استخدام التحليل المساعد على الاكتشاف للتحقق من صفحات الويب بحثاً عن الاحتيال وقم بتعيين مستوى تفاصيل الفحص.
 7. انقر فوق الزر 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 مركز الحماية.

4. في الجزء الأيمن من النافذة، في القسم طرق الفحص، حدد خانة الاختيار التحقق من وجود عناوين مواقع الويب في قاعدة بيانات عناوين المواقع الاحتمالية.

5. انقر فوق الزر تطبيق في النافذة الإعدادات.

لوحة المفاتيح الظاهرية

عند العمل على الإنترنت، عادة تحتاج إلى إدخال بياناتك الشخصية أو اسم المستخدم وكلمة المرور الخاصة بك. ويحدث هذا، على سبيل المثال، أثناء تسجيل حساب على مواقع ويب أو أثناء التسوق عبر الإنترنت أو إجراء أعمال بنكية عبر الإنترنت.

هناك خطر من اعتراض هذه المعلومات الشخصية عن طريق معترضي لوحات المفاتيح، أو برامج تسجل لوحة المفاتيح، وهي برامج تقوم بتسجيل نقرات لوحة مفاتيح الجهاز.

تمنع لوحة المفاتيح الظاهرية اعتراض البيانات المدخلة باستخدام لوحة المفاتيح.

تمنع لوحة المفاتيح الظاهرية اعتراض البيانات الخاصة فقط عند العمل مع مستعرضات Microsoft Internet Explorer و Mozilla™ 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 متوفرة في Microsoft Internet Explorer 10 في النمط Metro، وكذلك في Microsoft Internet Explorer 10 في حالة عدم تحديد خانة الاختيار تمكين الوضع المحمي المعزز في إعدادات المستعرض. في هذه الحالة، نوصيك بتفعيل لوحة المفاتيح الظاهرية من خلال واجهة Kaspersky Anti-Virus.

لا تستطيع لوحة المفاتيح الظاهرية حماية بياناتك الشخصية إذا تعرض الموقع، الذي يطلب إدخال هذه البيانات، لهجوم القرصنة، حيث إنه في هذه الحالة سيتم الحصول على المعلومات مباشرة عن طريق الدخلاء.

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 اعتراض البيانات الشخصية التي يتم إدخالها من خلال استخدام لقطات الشاشة.

لوحة المفاتيح الظاهرية لا تمنع من اتخاذ المزيد من صور لقطات الشاشة باستخدام مفتاح طباعة الشاشة ومجموعات أخرى من المفاتيح التي توفرها إعدادات نظام التشغيل، فضلا عن إنشاء لقطات باستخدام DirectX.

وتتميز لوحة المفاتيح الظاهرية بالميزات التالية:

- يمكنك النقر فوق أزرار لوحة المفاتيح الظاهرية باستخدام الماوس.
- بخلاف لوحات المفاتيح الحقيقية، لا توجد طريقة للنقر فوق مفاتيح في لوحة المفاتيح الظاهرية في وقت واحد. 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. تعمل النقرة الثانية للمفتاح بنفس الطريقة التي يعمل بها تحرير 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 التي يتم إدخالها من خلال لوحة المفاتيح الظاهرية، يجب إعادة تشغيل الكمبيوتر الخاص بك بعد أن يتم تثبيت Kaspersky Anti-Virus.

يمكنك فتح لوحة المفاتيح الظاهرية بالطرق التالية:

- من قائمة السياق الخاصة برمز التطبيق الموجود في منطقة إخطارات شريط المهام

- من نافذة التطبيق الرئيسية،
- استخدام خليط من المفاتيح على لوحة مفاتيح الكمبيوتر؛
- استخدم أداة برنامج Kaspersky Anti-Virus (فقط لنظامي التشغيل Microsoft Windows Vista و Microsoft Windows 7).
- ➔ لفتح لوحة المفاتيح الظاهرية من قائمة سياق رمز التطبيق في منطقة إخطارات شريك المهام،
- حدد لوحة المفاتيح الظاهرية من قائمة سياق رمز التطبيق (راجع الشكل الموجود أدناه).



الشكل 6. قائمة سياق رمز التطبيق

- ➔ لفتح لوحة المفاتيح الظاهرية من نافذة التطبيق الرئيسية:
- في الجزء السفلي من نافذة التطبيق الرئيسية، حدد القسم لوحة المفاتيح الظاهرية.
- ➔ لفتح لوحة المفاتيح الظاهرية باستخدام لوحة مفاتيح الكمبيوتر،
- اضغط الاختصار **CTRL+ALT+SHIFT+P**.
- ➔ لفتح لوحة المفاتيح الظاهرية باستخدام الأداة الذكية،
- انقر فوق زر الأداة الذكية التي تم تعيين هذا الإجراء إليها (راجع القسم "الذكاء Kaspersky أداة استخدام" على الصفحة 54).

منظف الخصوصية

- يتم تسجيل إجراءات المستخدم على الكمبيوتر في نظام التشغيل. يتم حفظ المعلومات التالية:
- تفاصيل بحث الاستعلامات التي يقوم المستخدمون ومواقع الويب بإدخالها
 - معلومات حول التطبيقات التي تم بدأ تشغيلها والملفات المفتوحة والمحفوظة
 - إدخال 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 Anti-Virus معالج منظف الخصوصية، الذي يقوم بتنظيف آثار نشاط المستخدم في النظام.

➔ **لبدء تشغيل معالج منظف الخصوصية:**

1. افتح نافذة التطبيق الرئيسية.
 2. في الجزء الأسفل من النافذة، حدد القسم **الأدوات**.
 3. في النافذة التي سيتم فتحها، في القسم **منظف الخصوصية**، انقر فوق الزر **ابدا**.
- يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يمكنك التنقل بينها باستخدام الزرين **السابق** و**التالي**. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**. لإيقاف المعالج في أي مرحلة، انقر الزر **إلغاء**.
- دعنا نفحص خطوات المعالج بالتفصيل.

1Step. بدء تشغيل المعالج

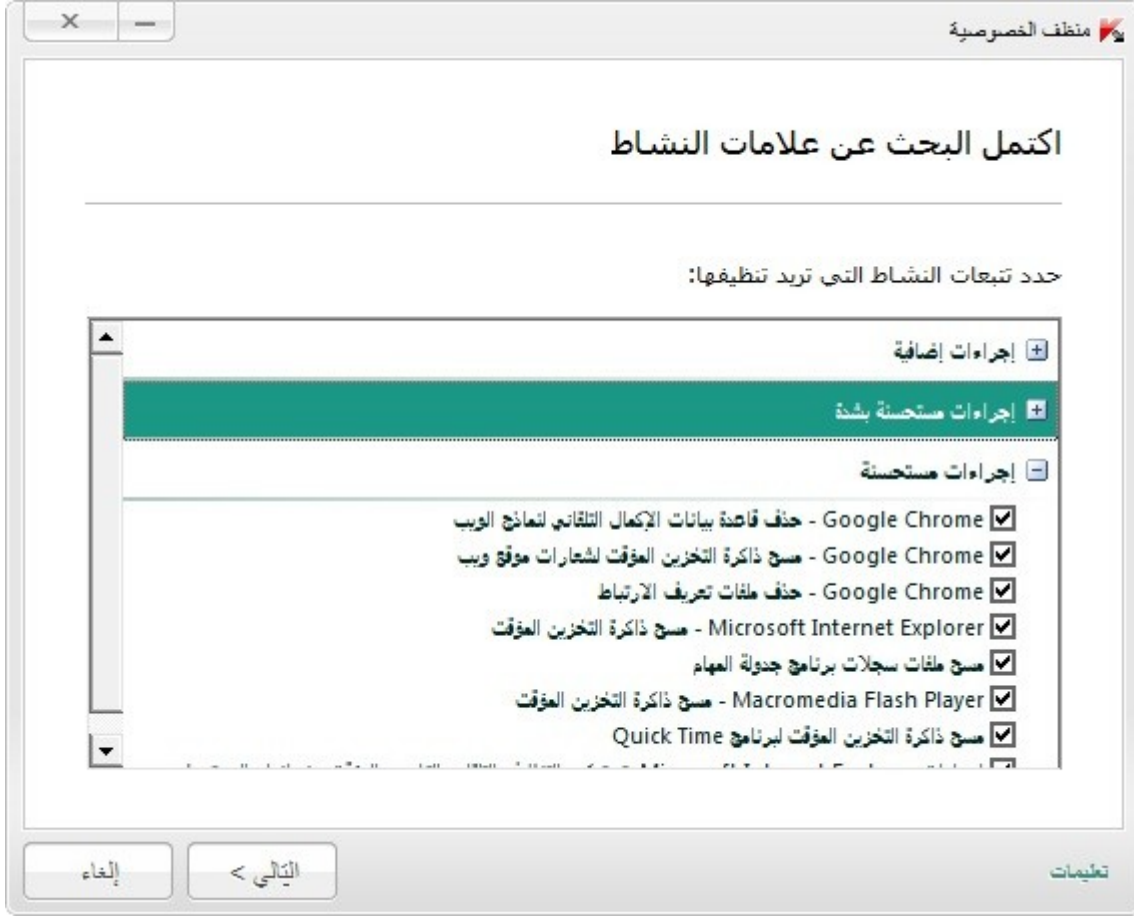
تأكد من تحديد الخيار **البحث عن تتبعات نشاط المستخدم**، وانقر فوق الزر **التالي** لبدء تشغيل المعالج.

2Step. البحث عن علامات النشاط

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

3Step. تحديد إجراءات منظف الخصوصية

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



الشكل 7. 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 المتوافق. وافترضياً، ينفذ المعالج جميع الإجراءات المستحسنة والمستحسنة بشدة. إذا لم ترغب في تنفيذ إجراء معين، قم بإلغاء تحديد المربع المجاور له.

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

بعد تحديد مجموعة الإجراءات التي سيقوم المعالج بتنفيذها، انقر الزر التالي.

4.Step. منظف الخصوصية

سينفذ المعالج الإجراءات المحددة أثناء الخطوة السابقة. وقد يستغرق التخلص من تتبعات النشاط بعض الوقت. لمسح تتبعات نشاط محدد، قد تكون هناك حاجة لإعادة التمهيد؛ في هذه الحالة سيقوم المعالج بإخطارك.

وبمجرد أن ينتهي البحث، ينتقل المعالج تلقائياً إلى الخطوة التالية.

5.Step. اكتمال المعالج

إذا كنت ترغب في تنظيف تتبعات نشاط المستخدم تلقائيًا كلما انتهى برنامج Kaspersky Anti-Virus من عمله، استخدم آخر شاشة للمعالج لتحديد خانة الاختيار **تنظيف تتبعات النشاط في كل مرة خروج من برنامج Kaspersky Anti-Virus**. وإذا كنت تخطط لإزالة تتبعات النشاط يدويًا باستخدام المعالج، لا تقم بتحديد خانة الاختيار هذه.




انقر الزر **إنهاء لإغلاق المعالج**.

تقييم الحالة الآمنة لموقع الويب

يسمح Kaspersky Anti-Virus بفحص موقع الويب للأمان قبل الانتقال إلى موقع الويب بواسطة الارتباط. لتنفيذ هذا الأمر، يتم استخدام وحدة نمطية يطلق عليها مستشار Kaspersky لعناوين مواقع الويب.

مستشار Kaspersky لعناوين مواقع الويب غير متوفر في **Microsoft Internet Explorer 10** في النمط **Metro**، وكذلك في **Microsoft Internet Explorer 10** في حالة عدم تحديد خانة الاختيار **تمكين الوضع المحمي المعزز في إعدادات المستعرض**.

يتم تكامل مستشار Kaspersky لعناوين مواقع الويب في مستعرضات Microsoft Internet Explorer و Google Chrome و Mozilla و Firefox، ويقوم بفحص الارتباطات الموجودة على صفحات الويب المفتوحة في المستعرض. يعرض Kaspersky Anti-Virus أحد الرموز التالية بجوار كل ارتباط:

- في حالة فتح صفحة الويب عن طريق النقر فوق الارتباط تكون الصفحة آمنة وفقًا لـ Kaspersky Lab 
- في حالة عدم وجود معلومات حول حالة سلامة صفحة الويب المفتوحة عن طريق النقر فوق الارتباط 
- في حالة فتح صفحة الويب عن طريق النقر فوق الارتباط تكون الصفحة 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 Anti-Virus 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 الزر **إعدادات**.
- سيتم فتح النافذة **مكافحة فيروسات الويب**.
4. في النافذة التي يتم فتحها، على علامة التبويب **التصفح الآمن**، في قسم **مستشار Kaspersky لعناوين مواقع الويب** انقر فوق الزر **إعدادات**.
- سيتم فتح النافذة **إعدادات مستشار Kaspersky لعناوين مواقع الويب**.
5. في النافذة التي سيتم فتحها، في القسم **وضع الفحص** حدد جميع ارتباطات URL.
6. انقر فوق الزر **تطبيق** في النافذة **الإعدادات**.

استخدام ملف تعريف الألعاب لوضع ملء الشاشة

عندما يتم تشغيل Kaspersky Anti-Virus بالتزامن مع بعض التطبيقات (بالأخص ألعاب الفيديو)، قد تحدث الحالات السلبية التالية في وضع ملء الشاشة:

- انخفاض أداء التطبيق أو اللعبة بسبب عدم توفر موارد النظام
- تؤدي نوافذ الإخطارات الخاصة بـ Kaspersky Anti-Virus إلى تشتيت انتباه المستخدم عن اللعب.

لتجنب تغيير إعدادات Kaspersky Anti-Virus يدويًا في كل مرة يتم فيها التحويل إلى وضع ملء الشاشة، يمكنك استخدام ملف بيانات الألعاب. عندما يكون ملف بيانات الألعاب ممكنًا، فإن التبديل إلى وضع ملء الشاشة يغير تلقائيًا إعدادات جميع مكونات Kaspersky Anti-Virus لضمان تشغيل النظام المثالي في هذا الوضع. بمجرد الخروج من وضع ملء الشاشة، تعود إعدادات المنتج إلى القيم الأولية قبل إدخال وضع ملء الشاشة.

► لتمكين ملف بيانات الألعاب:

1. افتح نافذة إعدادات التطبيق.
2. في الجزء الأيمن من النافذة، في القسم إعدادات متقدمة، حدد القسم الفرعي ملف الألعاب.
3. حدد خانة الاختيار استخدام ملف بيانات الألعاب وحدد إعدادات ملف بيانات الألعاب الضرورية في القسم خيارات ملف البيانات أدناه.

إنشاء قرص الإنقاذ واستخدامه

يعتبر قرص الإنقاذ عبارة عن تطبيق باسم قرص إنقاذ Kaspersky ويتم تسجيله على وسيط قابل للإزالة (القرص المضغوط أو محرك فلاش USB).

وستكون لديك القدرة كذلك على استخدام قرص إنقاذ Kaspersky في فحص أجهزة الكمبيوتر المصابة وتنظيفها التي يتعذر تنظيفها باستخدام الطرق الأخرى (على سبيل المثال، باستخدام تطبيقات مكافحة الفيروسات).

في هذا القسم:

47 الإنقاذ قرص إنشاء

49 الإنقاذ قرص باستخدام الكمبيوتر على

إنشاء قرص الإنقاذ

يتضمن إنشاء قرص إنقاذ تكوين صورة قرص (ملف ISO) باستخدام أحدث إصدار من قرص إنقاذ Kaspersky وحفظه على محرك أقراص قابل للإزالة.

يمكنك تحميل صورة القرص الأصلية من خادم Kaspersky Lab أو نسخه من المصدر المحلي.

يتم إنشاء قرص الإنقاذ باستخدام معالج إنشاء قرص إنقاذ 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 و Microsoft Windows 7 – في المجلد التالي: ProgramData\Kaspersky .\Lab\AVP13\Data\Rdisk

➔ لتشغيل معالج إنشاء قرص إنقاذ Kaspersky:

1. افتح نافذة التطبيق الرئيسية.
 2. في الجزء الأسفل من النافذة، حدد القسم الأدوات.
 3. في النافذة التي سيتم فتحها، في القسم قرص إنقاذ Kaspersky، انقر فوق الزر فتح.
- يتألف المعالج من سلسلة من الشاشات (الخطوات) التي يمكنك التنقل بينها باستخدام الزرين السابق والتالي. لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر إنهاء. لإيقاف المعالج في أي مرحلة، انقر الزر إلغاء.
- دعنا نفحص خطوات المعالج بالتفصيل.

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

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

إذا اكتشف المعالج وجود ملف ISO لقرص الإنقاذ في المجلد المخصص (انظر أعلاه)، سيظهر المربع استخدام صورة ISO الموجودة في النافذة الأولى للمعالج. حدد خانة الاختيار المطلوبة لاستخدام الملف المكتشف كصورة ISO أصلية ثم انتقل مباشرة إلى الخطوة تحديث صورة القرص (انظر أدناه). قم بمسح خانة الاختيار هذه إذا كنت لا ترغب في استخدام صورة القرص التي تم اكتشافها. سيتابع المعالج إلى النافذة تحديد مصدر صورة القرص.

2Step. تحديد مصدر صورة القرص

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

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

- إذا قمت بالفعل بتسجيل نسخه من قرص الإنقاذ أو صورة ISO المحفوظة على الكمبيوتر الخاص بك أو على مورد محلي آخر، حدد الخيار نسخ صورة ISO من محرك أقراص محلي أو على الشبكة.
- إذا لم يكن لديك ملف صورة ISO تم إنشائه لقرص الإنقاذ، وترغب في تنزيل واحد من خادم Kaspersky Lab (يل حجم الملف إلى حوالي 175 ميجا بايت)، حدد تحميل صورة ISO من خادم Kaspersky Lab.

3Step. نسخ (تحميل) صورة القرص

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

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

إذا قمت بتحديد تحميل 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.

4Step. تحديث ملف صورة ISO

يتكون إجراء تحديث ملف صورة ISO من العمليات التالية:

- تحديث قواعد بيانات التطبيق.
- تحديث ملفات التكوين.

تحدد ملفات التكوين ما إذا كان يمكن تمهيد الكمبيوتر من وسيط قابل للإزالة (مثل CD / DVD أو محرك أقراص فلاش USB) باستخدام قرص إنقاذ (Kaspersky) تم إنشاؤه بواسطة المعالج.

عند تحديث قواعد بيانات التطبيقات، يتم استخدام تلك التي تم توزيعها في آخر تحديث لبرنامج Kaspersky Anti-Virus. إذا كانت قواعد البيانات قديمة، يوصى بتشغيل مهمة التحديث وتشغيل معالج إنشاء قرص إنقاذ Kaspersky مرة أخرى.

لبدء تحديث ملف ISO، انقر الزر التالي. سيتم عرض تقدم التحديث في نافذة المعالج.

5Step. تسجيل صورة القرص على وسيط

عند هذه الخطوة، يخبرك المعالج بنجاح إنشاء صورة القرص ويعرض عليك تسجيله على وسيط بيانات.

حدد وسيط بيانات لتسجيل قرص إنقاذ Kaspersky:

- لتسجيل صورة القرص على قرص مضغوط أو قرص DVD، حدد التسجيل على قرص DVD / CD وحدد الجهاز الذي ترغب في تسجيل صورة القرص عليه.
- لتسجيل صورة القرص على محرك فلاش USB، حدد التسجيل على محرك أقراص فلاش USB وحدد الجهاز الذي ترغب في تسجيل صورة القرص عليه.

توصي شركة Kaspersky Lab بعدم تسجيل صورة ISO على أجهزة غير مصممة خصيصًا لتخزين البيانات، مثل الهواتف الذكية والهواتف الخلوية وأجهزة PDA ومشغلات 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.

6Step. اكتمال المعالج

لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر إنهاء. يمكنك استخدام قرص الإنقاذ الذي تم إنشاؤه حديثًا من أجل تمهيد الكمبيوتر (رجع الصفحة 49) إذا لم تتمكن من تمهيده وتشغيل Kaspersky Anti-Virus في الوضع الطبيعي بسبب وجود تأثير بسبب الفيروسات أو البرمجيات الخبيثة.

بدء تشغيل الكمبيوتر باستخدام قرص الإنقاذ

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

لتمهيد نظام التشغيل، يجب عليك استخدام قرص مضغوط / قرص DVD أو محرك فلاش USB مع قرص إنقاذ Kaspersky المنسوخ عليه (راجع القسم "إنقاذ قرص إنقاذ" على الصفحة 47).

لا يكون تمهيد الكمبيوتر من وسيط بيانات قبل للإزالة أمرًا ممكنًا في جميع الأحيان. وبوجه خاص، لا تدعم بعض الطرازات القديمة لأجهزة الكمبيوتر هذا الوضع. وقبل إيقاف تشغيل الكمبيوتر للقيام بالتمهيد لاحقًا من وسيط أقراص قابل للإزالة، تأكد من أنه يمكن تنفيذ هذا التشغيل.

1. في إعدادات BIOS، قم بتمكين التمهيد من CD / DVD أو من جهاز USB (للحصول على معلومات تفصيلية، برجاء الرجوع إلى الوثائق الخاصة باللوحة الأم للكمبيوتر الخاص بك).
2. قم بإدراج قرص مضغوط / قرص DVD في محرك الأقراص المضغوطة / أقراص DVD لكمبيوتر مصاب أو قم بتوصيل جهاز USB تم نسخ قرص إنقاذ Kaspersky عليه.
3. أعد تشغيل الكمبيوتر.

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

تقييد الوصول إلى برنامج KASPERSKY ANTI-VIRUS باستخدام كلمة المرور

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

ولتقييد الوصول إلى التطبيق، يمكنك تعيين كلمة مرور مسؤول وتحديد الإجراءات المطلوبة لإدخال كلمة المرور:

- تكوين إعدادات التطبيق
- إغلاق التطبيق؛
- إزالة التطبيق.

للوصول المحمي بكلمة المرور إلى برنامج Kaspersky Anti-Virus

1. افتح نافذة التطبيق الرئيسية.
2. في الركن الأيسر العلوي من النافذة، انقر فوق الارتباط الإعدادات.
3. في النافذة الإعدادات التي سيتم فتحها، حدد القسم الفرعي إعدادات عامة في القسم مركز الحماية.
4. حدد خانة الاختيار إعدادات التطبيق المحمي بكلمة مرور وانقر فوق الزر إعدادات.
- سيتم فتح النافذة الحماية بكلمة مرور.
5. في النافذة التي سيتم فتحها، قم بإكمال الحقلين كلمة المرور الجديدة و تأكيد كلمة المرور.
6. لتغيير كلمة مرور تم إنشاؤها من قبل، اكتبها في الحقل كلمة المرور القديمة.
7. ضمن مجموعة الإعدادات تطبيق كلمة المرور على، حدد العمليات الخاصة بالتطبيقات والتي يجب حماية الوصول إليها باستخدام كلمات المرور.
8. انقر فوق الزر تطبيق في النافذة الإعدادات.

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

إيقاف حماية الكمبيوتر واستعادتها

يعني الإيقاف المؤقت للحماية تعطيل 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 8. 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** – سوف يتم تمكين الحماية بعد انتهاء الفاصل الزمني المحدد في القائمة المنسدلة الموجودة أدناه.
- **إيقاف مؤقت حتى إعادة التمهيد** – سيتم تمكين الحماية بعد إعادة تشغيل التطبيق أو إعادة تمهيد نظام التشغيل (بشرط تمكين بدء تشغيل التطبيق التلقائي).
- **الإيقاف المؤقت** – ستتم متابعة الحماية بعد أن تقرر أنت متابعتها.

➔ لاستئناف حماية الكمبيوتر،

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

عرض تقرير تشغيل التطبيق

يحافظ Kaspersky Anti-Virus على تقارير التشغيل لكل مكون من مكونات الحماية. باستخدام تقرير، يمكنك الحصول على معلومات إحصائية حول تشغيل التطبيق (على سبيل المثال، تعلم كيفية اكتشاف الكثير من الكائنات الخبيثة وإبطالها خلال فترة زمنية محددة، وكم عدد المرات تحديث التطبيق خلال نفس الفترة، وعدد رسائل البريد غير المرغوب فيها التي تم اكتشافها والمزيد).

عند العمل على جهاز كمبيوتر يعمل بنظام Microsoft Windows Vista أو Microsoft Windows 7، يمكنك فتح تقارير باستخدام Kaspersky Gadget. وللقيام بذلك، يجب تكوين Kaspersky Gadget بحيث يتم تعيين خيار فتح نافذة التقارير لأحد أزراره (انظر القسم "Kaspersky Gadget" استخدام ك ي ف ية" في صفحة 54).

➔ لعرض تقرير تشغيل التطبيق:

1. افتح النافذة **التقارير** باستخدام واحدة من الطرق التالية:
 - انقر الارتباط **التقارير** في الجزء العلوي من نافذة التطبيق الرئيسية
 - انقر الزر الذي به الرمز **التقارير** في واجهة Kaspersky Gadget (فقط بالنسبة لنظامي التشغيل Microsoft Windows Vista و Microsoft Windows 7).تظهر تقارير حماية التطبيق كرسومات بيانية في النافذة **التقارير**.
 2. إذا رغبت في عرض تقرير مفصل حول نشاط التطبيق (على سبيل المثال، تقرير يعرض نشاط كل مكون)، انقر فوق الزر **تقرير تفصيلي** في الجزء السفلي من النافذة **التقرير**.
- تفتح النافذة **تقرير تفصيلي** في المكان الذي تعرض فيه البيانات في جدول. ولسهولة عرض التقارير، يمكنك تحديد العديد من خيارات فرز الإدخال.

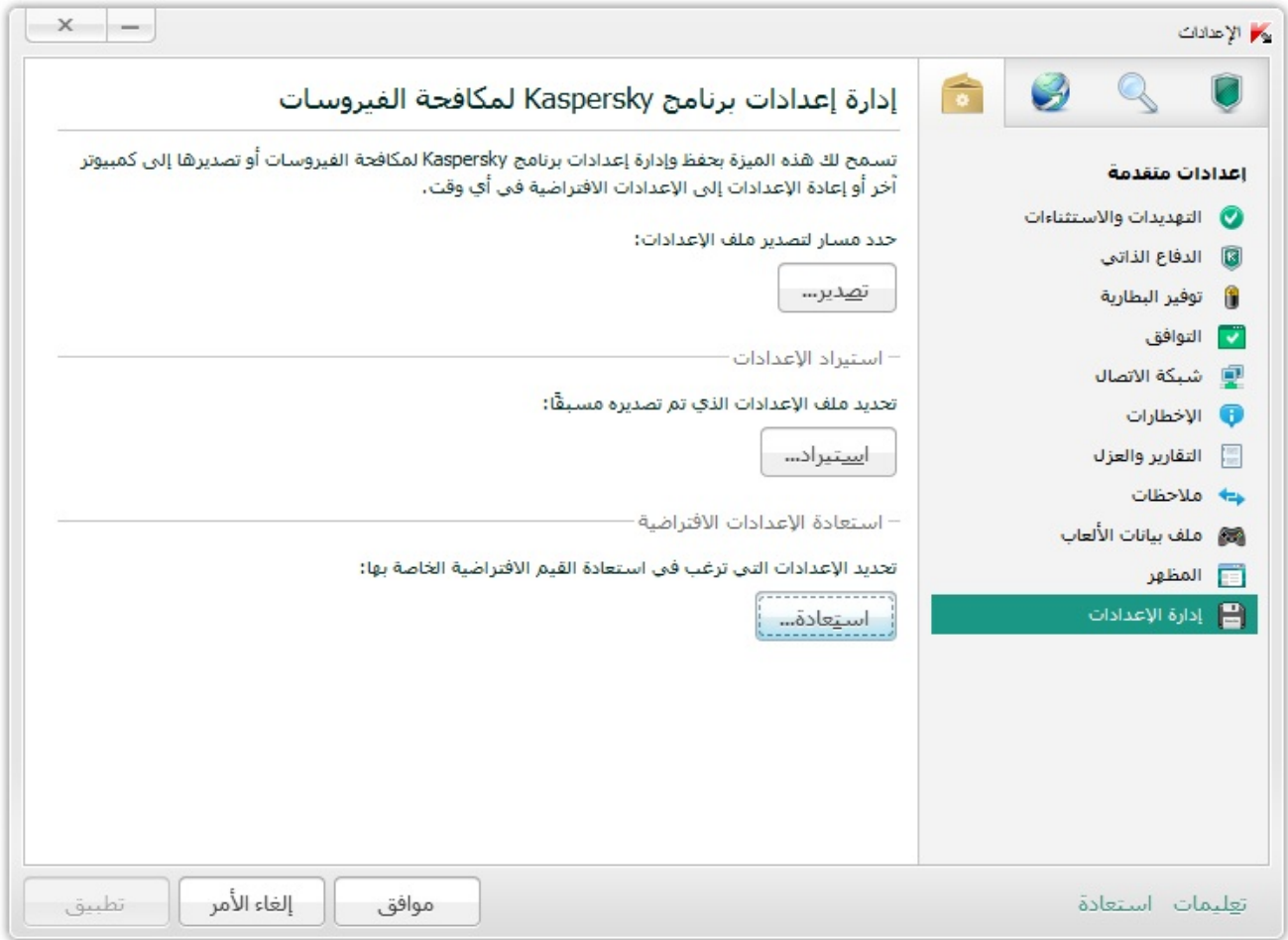
استعادة إعدادات التطبيق الافتراضية.

يمكنك استعادة إعدادات التطبيق الافتراضية الموصى بها من قبل Kaspersky Lab لبرنامج Kaspersky Anti-Virus في أي وقت. ويمكن استعادة الإعدادات باستخدام **معالج تكوين التطبيق**. عندما يكمل المعالج العملية الخاصة به، يتم ضبط مستوى الأمان **مستحسن** لجميع مكونات الحماية. عند استعادة مستوى الأمان الموصى به، يمكنك حفظ القيم المحددة مسبقاً لبعض إعدادات مكونات التطبيق.

➔ لتشغيل معالج تكوين التطبيق:

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

- في الركن العلوي من النافذة، حدد القسم إعدادات متقدمة، وحدد القسم الفرعي إدارة الإعدادات وانقر فوق الزر استعادة في القسم استعادة الإعدادات الافتراضية (راجع الشكل الموجود أدناه).



الشكل 9. النافذة إعدادات، القسم الفرعي إدارة الإعدادات

دعنا نفحص خطوات المعالج بالتفصيل.

1.Step. بدء تشغيل المعالج

انقر الزر التالي لمتابعة التنصيب.

2.Step. استعادة الإعدادات

تعرض نافذة المعالج هذه مكونات برنامج Kaspersky Anti-Virus التي تختلف إعداداتها عن القيمة الافتراضية، بسبب أنها تم تغييرها من قبل المستخدم. في حالة إنشاء إعدادات خاصة لأي من المكونات، سيتم إظهارها أيضاً في النافذة (راجع الشكل الموجود أدناه).

حدد خانة الاختيار الخاصة بالإعدادات التي ترغب في حفظها وانقر الزر التالي.

3.Step. إنهاء الاستعادة

لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر إنهاء.

استيراد إعدادات التطبيق إلى KASPERSKY ANTI-VIRUS المثبت على كمبيوتر آخر

بمجرد إتمام تهيئة المنتج، يمكنك تطبيق إعداداته في برنامج Kaspersky Anti-Virus المثبت على جهاز كمبيوتر آخر. وبالتالي، سيتم تكوين التطبيق بشكل متماثل على كلا جهازي الكمبيوتر. هذه الميزة مفيدة عندما يكون برنامج Kaspersky Anti-Virus مثبت بجهاز الكمبيوتر بالمنزل أو بالمكتب على سبيل المثال.

يمكن نقل إعدادات Kaspersky Anti-Virus إلى كمبيوتر آخر خلال ثلاث خطوات:

1. تصدير إعدادات التطبيق إلى ملف التكوين.
2. نقل ملف التكوين إلى كمبيوتر آخر (على سبيل المثال، عن طريق البريد الإلكتروني أو على وسيطة قابلة للإزالة).
3. تطبيق الإعدادات من ملف التكوين على التطبيق المثبت على كمبيوتر مختلف.

➔ لحفظ إعدادات Kaspersky Anti-Virus إلى ملف التكوين:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط الإعدادات في الجزء العلوي من النافذة.
3. في الجزء العلوي من النافذة الإعدادات في القسم الإعدادات المتقدمة حدد القسم الفرعي إدارة الإعدادات.
4. انقر فوق الزر تصدير في القسم الفرعي إدارة الإعدادات.
5. في النافذة التي ستفتح، أدخل اسم ملف التكوين وحدد الموقع الذي يجب حفظه فيه.
6. انقر فوق موافق.

➔ لتطبيق الإعدادات من ملف التكوين على التطبيق المثبت على كمبيوتر مختلف:

1. افتح نافذة التطبيق الرئيسية.
2. انقر الارتباط الإعدادات في الجزء العلوي من النافذة.
3. في الجزء العلوي من النافذة الإعدادات في القسم الإعدادات المتقدمة حدد القسم الفرعي إدارة الإعدادات.
4. انقر فوق الزر استيراد في القسم الفرعي إدارة الإعدادات.
5. في النافذة التي ستفتح، قم بتحديد الملف الذي ترغب في استيراد إعدادات برنامج Kaspersky Anti-Virus منه.
6. انقر فوق موافق.

استخدام أدوات KASPERSKY الذكية

عند استخدام برنامج Kaspersky Anti-Virus على جهاز كمبيوتر يعمل بنظام Microsoft Windows Vista أو Microsoft Windows 7، يمكنك استخدام Kaspersky Gadget أيضاً (يشار إليها فيما يلي بالأدوات الذكية). بعد قيامك بتنصيب برنامج Kaspersky Anti-Virus على جهاز كمبيوتر يعمل بنظام Microsoft Windows 7، تظهر الأداة على سطح المكتب تلقائياً. وبعد قيامك بتنصيب التطبيق على جهاز كمبيوتر يعمل بنظام Microsoft Windows Vista، يجب أن تقوم بإضافة الأداة إلى Microsoft Windows Sidebar يدوياً (انظر وثائق نظام التشغيل).

يعرض مؤشر لون الأداة الذكية حالة حماية الكمبيوتر الخاص بك بنفس الطريقة المتبعة مع المؤشر الموجود في نافذة التطبيق الرئيسية (راجع القسم "الأمان المتعلقة بمشاكل وحل الكمبيوتر بحماية حالة تقييم" على الصفحة 31). يشير اللون الأخضر إلى أن جهاز الكمبيوتر محمي كما ينبغي، بينما يشير اللون الأصفر إلى وجود مشكلات تتعلق بالحماية، كما يشير اللون الأحمر إلى أن أمان الكمبيوتر في خطر شديد. ويشير اللون الرمادي إلى توقف التطبيق.

يمكنك استخدام الأداة لأداء الإجراءات التالية:

- متابعة التطبيق في حالة إيقافه مؤقتًا سابقًا؛
- فتح نافذة التطبيق الرئيسية
- فحص كائنات محددة للبحث عن فيروسات
- فتح نافذة الأخبار

كما يمكنك أيضًا تكوين الأزرار الموجودة على الأداة لتقوم بتهيئة الإجراءات الإضافية:

- تشغيل تحديث؛
- تحرير إعدادات التطبيق؛
- عرض تقارير التطبيق؛
- إيقاف الحماية مؤقتًا؛
- فتح لوحة المفاتيح الظاهرية
- فتح نافذة إدارة المهام.

➔ لبدء تشغيل التطبيق باستخدام الأداة،

انقر الرمز  تمكين الموجود في وسط الأداة.

➔ لفتح نافذة التطبيق الرئيسية باستخدام الأداة


انقر فوق رمز الشاشة الموجود في المنطقة المركزية للأداة الذكية.

➔ لفحص كائن للبحث عن الفيروسات باستخدام الأداة


اسحب الكائن المطلوب فحصه على الأداة.

سيتم عرض تقدم المهمة في النافذة إدارة المهام.

➔ لفتح نافذة الأخبار باستخدام الأداة

انقر الرمز  الذي يظهر في وسط الأداة عند إصدار أحد الأخبار.

➔ لتكوين الأداة

1. افتح نافذة إعدادات الأداة الذكية عن طريق النقر فوق الرمز  الذي سيطهر في الركن الأيسر العلوي من كتلة الأداة الذكية إذا قمت بوضع المؤشر فوقه.

2. في القائمة المنسدلة المقابلة لأزرار الأداة الذكية، حدد الإجراءات التي يجب أن تقوم بتنفيذها عندما تقوم بالنقر فوق هذه الأزرار.

المشاركة في شبكة أمان (KASPERSKY (KSN

لزيادة فاعلية حماية الكمبيوتر الخاص بك، يستخدم Kaspersky Anti-Virus بيانات تم استلامها من مستخدمين من جميع أنحاء العالم. تم تصميم شبكة أمان Kaspersky لتجميع هذه البيانات.

تعتبر شبكة أمان (Kaspersky (KSN هي بنية أساسية من خدمات الإنترنت التي توفر الوصول إلى قاعدة معلومات Kaspersky Lab عبر الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويضمن استخدام البيانات من شبكة أمان Kaspersky زيادة وقت الاستجابة من تطبيقات Kaspersky Anti-Virus عند مواجهة أنواع جديدة من التهديدات، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية والتقليل من خطر الحالات الإيجابية الخاطئة.

وبفضل المستخدمين المشاركين في شبكة أمان Kaspersky، يستطيع Kaspersky Lab تجميع المعلومات بسرعة حول أنواع ومصادر التهديدات الجديدة وتطوير حلول حول إبطالها وتقليل عدد الحالات الإيجابية الخاطئة. تسمح لك المشاركة في شبكة أمان Kaspersky بالوصول إلى إحصائيات سمعة التطبيقات ومواقع الويب.

في هذا القسم:

وتعطيلها Kaspersky أمان شبكة في المشاركة تمكين 56

56 Kaspersky أمان شبكة الاتصال فحص

تمكين المشاركة في شبكة أمان KASPERSKY وتعطيلها

المشاركة الاختيارية في شبكة أمان Kaspersky. يمكنك تمكين أو تعطيل استخدام شبكة أمان Kaspersky عند تثبيت Kaspersky Anti-Virus و / أو في أي لحظة بعد تثبيت التطبيق.

تمكين المشاركة في شبكة أمان Kaspersky أو تعطيلها:

1. افتح نافذة التطبيق الرئيسية.
 2. انقر الارتباط الإعدادات في الجزء العلوي من النافذة.
 3. في النافذة الإعدادات التي ستفتح، في القسم الإعدادات المتقدمة، حدد القسم الفرعي التعليقات.
 4. في الجزء الأيسر من النافذة، نفذ أي مما يلي:
- إذا كنت ترغب في المشاركة في KSN، حدد خانة الاختيار أوافق على المشاركة في شبكة أمان Kaspersky.
 - إذا كنت ترغب في المشاركة في KSN، قم بإلغاء تحديد خانة الاختيار أوافق على المشاركة في شبكة أمان Kaspersky.

فحص الاتصال بشبكة أمان KASPERSKY

قد يتم فقد الاتصال مع شبكة أمان Kaspersky للأسباب التالية:

- أنت لا تشارك في شبكة اتصال أمان Kaspersky

- الكمبيوتر الخاص بك غير متصل بالإنترنت.
- حالة المفتاح الحالي لا تسمح بالاتصال بشبكة أمان Kaspersky.

يتم عرض حالة المفتاح الحالية في النافذة التراخيص (راجع القسم "وتجديده الـ" [ترخيص على الـ صول](#)" على الصفحة 30).

➔ لفحص الاتصال بشبكة أمان Kaspersky:

1. افتح نافذة التطبيق الرئيسية.
 2. انقر الارتباط الحماية السحابية في الجزء العلوي من النافذة.
- في الجزء الأيمن من النافذة التي سيتم فتحها، يتم عرض حالة الاتصال بشبكة أمان Kaspersky.

كيفية التبديل من برنامج Kaspersky Anti-Virus إلى برنامج Kaspersky Internet Security

يتيح لك برنامج Kaspersky Anti-Virus التبديل إلى Kaspersky Internet Security بدون أي تنزيلات أو تنبيلات إضافية للبرامج. برنامج Kaspersky لأمان الإنترنت هو عبارة عن تطبيق تم تصميمه لضمان توفير حماية شاملة لجهاز الكمبيوتر. وهو يوفر مجموعة كاملة من الميزات المتقدمة التي يتم تطبيقها مع الوحدات والوظائف التالية:

- التحكم في التطبيق
- الرقابة الأسرية؛
- جدار الحماية
- حاجب هجمات شبكة الاتصال
- الخدمات النقدية الأمانة
- عامل التصفية الجغرافي
- منع الوصول إلى مواقع الويب الخطرة
- مراقبة شبكة الاتصال
- مكافحة البريد الإلكتروني غير المرغوب فيه
- مكافحة الشعارات.

يمكنك التبديل مؤقتًا إلى الإصدار التجريبي من برنامج Kaspersky Internet Security للتعرف على مزاياه، أو البدء على الفور في استخدام الإصدار التجاري من التطبيق.

إذا استخدمت التطبيق باشتراك أو كنت تتعامل مع التطبيق في مناطق محددة، فإن نسخة Kaspersky Internet Security لا تتيح التبديل المؤقت إلى الإصدار التجريبي.

58 التجريبي الإصدار إلى مؤقتًا التبدل

59 التجريبي الإصدار إلى التبدل

التبديل مؤقتًا إلى الإصدار التجريبي

يمكنك التبديل مؤقتًا إلى الإصدار التجريبي من Kaspersky Internet Security من أجل تجريب وظائفه. بعد ذلك، يمكنك أيضًا شراء ترخيص لاستخدام التطبيق لاحقًا.

➔ للتبديل مؤقتًا إلى برنامج Kaspersky لأمان الإنترنت:

1. افتح نافذة التطبيق الرئيسية.
 2. في الجزء السفلي من النافذة، حدد القسم تحديث.
 3. في النافذة التي ستفتح، انقر الزر الإصدار التجريبي.
- يبدأ تشغيل معالج النقل.

إذا استخدمت التطبيق باشتراك أو كنت تتعامل مع التطبيق في مناطق محددة، فإن نسخة Kaspersky Internet Security لا تتيح التبديل المؤقت إلى الإصدار التجريبي. وفي تلك الحالات لا يظهر قسم تحديث في نافذة التطبيق الرئيسية.

دعنا نفحص خطوات المعالج بالتفصيل.

1.Step طلب تفعيل الإصدار التجريبي من برنامج Kaspersky Internet Security

في حالة إرسال طلب تنشيط Kaspersky Internet Security بنجاح، سيقوم المعالج بالمتابعة التلقائية إلى الخطوة التالية.

2.Step بدء التحديث

في هذه الخطوة، يعرض المعالج رسالة على الشاشة تبلغك بتوافر كافة المتطلبات المسبقة للنقل. ولمتابعة عمل المعالج، انقر الزر التالي.

3.Step إزالة التطبيقات غير المتوافقة

في هذه الخطوة، يتحقق المعالج من وجود أي تطبيقات غير متوافقة مع برنامج Kaspersky لأمان الإنترنت مثبتة على جهاز الكمبيوتر. إذا لم يتم العثور على تلك التطبيقات، سيتابع المعالج تلقائيًا إلى الخطوة التالية. في حالة العثور على مثل تلك التطبيقات، يسردها المعالج في النافذة ويعرض عليك إلغاء تثبيتها.

بعد أن يتم إلغاء تثبيت التطبيقات غير المتوافقة، قد تحتاج إلى إعادة تشغيل نظام التشغيل. بعدما يعاد بدء نظام التشغيل، يفتح المعالج تلقائيًا لاستئناف النقل.

4.Step التبديل إلى Kaspersky Internet Security

في هذه الخطوة، يتصل المعالج بمكونات Kaspersky Internet Security وهو ما قد يستغرق بعض الوقت. عندما تكتمل العملية، ينتقل المعالج تلقائيًا إلى الخطوة التالية.

5Step. إعادة تشغيل التطبيق

في الخطوة الأخيرة من النقل، يعاد تشغيل التطبيق. وللقيام بذلك، انقر الزر **إنهاء** في نافذة المعالج.

6Step. استكمال التفعيل

بعدما يعاد تشغيل التطبيق، يفتح المعالج تلقائياً. بعد نجاح تنشيط الإصدار التجريبي من Kaspersky Internet Security ، تعرض نافذة المعالج معلومات عن المدة التي يمكن خلالها استخدام الإصدار التجريبي.

7Step. تحليل النظام

يتم في هذه المرحلة جمع معلومات حول تطبيقات Microsoft Windows. تتم إضافة هذه التطبيقات إلى قائمة التطبيقات الموثوقة التي لا تحتوي على أي قيود مفروضة على الإجراءات التي تنفذها في النظام.

وبمجرد اكتمال التحليل، ينتقل المعالج تلقائياً إلى الخطوة التالية.

8Step. استكمال النقل

لإغلاق المعالج بمجرد إتمام مهمته، انقر الزر **إنهاء**.

لا يمكن تحويل التطبيق إلى الإصدار التجريبي من Kaspersky Internet Security لمرّة ثانية.

التبديل إلى الإصدار التجاري

إذا كنت تريد التبديل إلى الإصدار التجاري من Kaspersky Internet Security، فسوف تحتاج إلى رمز تفعيل للإصدار التجاري من التطبيق حتى يمكنك استخدامه في تنشيطه (راجع القسم "التطبيق يُلْتَفَع" على الصفحة 29).

➔ **شراء رمز تنشيط لبرنامج Kaspersky Internet Security:**

1. افتح نافذة التطبيق الرئيسية.
2. في الجزء السفلي من النافذة، حدد القسم **تحديث**.
3. في النافذة التي ستفتح، انقر فوق الزر **شراء رمز التنشيط**.

يعاد توجيهك إلى موقع المتجر الإلكتروني حيث يمكنك شراء رمز تنشيط لبرنامج Kaspersky Internet Security.

إذا استخدمت التطبيق باشتراك أو كنت تتعامل مع التطبيق في مناطق محددة، فإن نسخة Kaspersky Internet Security لا تتيح التبديل المؤقت إلى الإصدار التجريبي. وفي تلك الحالات لا يظهر قسم **تحديث** في نافذة التطبيق الرئيسية.

الاتصال بخدمة الدعم الفني

يوفر هذا القسم معلومات حول كيفية الحصول على الدعم الفني والمتطلبات الخاصة بالحصول على التعليمات من خدمة الدعم الفني.

في هذا القسم:

- 60 كيفية الحصول على الدعم الفني
- 60 الهاتف عبر الدعم الفني
- 60 Kaspersky في حسابي خلال من الدعم الفني على الحصول
- 62 AVZ وبرنامج التتبع ملف استخدام

كيفية الحصول على الدعم الفني

إذا لم تجد حلاً للمشكلة التي تواجهك في وثائق التطبيق أو في أحد مصادر المعلومات الخاصة بالتطبيق (راجع القسم " صادم بال تطبيق الخاصة بالمعلومات" على الصفحة 9)، نوصيك بالاتصال بخدمة الدعم الفني لـ Kaspersky Lab. وسوف يجيب أخصائيو خدمات 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. تسمح لك هذه الطريقة بالاتصال 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 بالمختصين من الدعم الفني باللغة الروسية أو الدعم الفني العالمي عبر الهاتف (http://support.kaspersky.com/support/international_local).

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

الحصول على الدعم الفني من خلال حسابي في KASPERSKY

يعتبر حسابي في Kaspersky 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:

- اتصل بخدمة الدعم الفني ومعمل الفيروسات.
- اتصل بخدمة الدعم الفني بدون استخدام البريد الإلكتروني.
- تتبع حالة الطلبات الخاصة بك في الوقت الحقيقي.
- عرض السجل التفصيلي لطلبات الدعم الفني.
- استلام نسخة من ملف المفتاح في حالة فقدته أو حذفه.

الدعم الفني باستخدام البريد الإلكتروني

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

في الحقول الخاصة بنموذج الطلب عبر الإنترنت، حدد البيانات التالية:

- نوع الطلب
- اسم التطبيق ورقم الإصدار
- وصف الطلب
- معرف 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 مكافحة الفيروسات بدلاً من خدمة الدعم الفني.

يمكنك إرسال طلبات الأنواع التالية إلى معمل الفيروسات:

- برنامج خبيث غير معروف – تشك في أن الملف يحتوي على فيروس ولكن لم يتم Kaspersky Anti-Virus بتحديد كملف مصاب.
- يقوم المتخصصين في معمل مكافحة الفيروسات بتحليل الرمز الخبيث المرسل. إذا اكتشفوا فيروساً مجهولاً من قبل، فإنهم يقومون بإضافة وصف متطابق إلى قاعدة البيانات والذي يصبح متاحاً عند تحديث تطبيقات مكافحة الفيروسات.
- إنذار زائف – يقوم Kaspersky Anti-Virus بتصنيف الملف على أنه فيروس ولكنك متأكدًا من أن هذا الملف ليس فيروساً.
- طلب وصف البرنامج الخبيث – أنت تريد استقبال وصف لفيروس اكتشفه Kaspersky Anti-Virus باستخدام اسم 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.

استخدام ملف التتبع وبرنامج AVZ النصي

بعد أن تقوم بإخطار المتخصصين في خدمة الدعم الفني بالمشكلة التي واجهتك، قد يطالبونك بإنشاء تقرير يضم معلومات حول نظام التشغيل الخاص بك وإرسال التقرير إلى خدمة الدعم الفني. كما قد يطلب منك المتخصصون في خدمة الدعم الفني أيضًا إنشاء ملف تتبع. يسمح لك ملف التتبع بتتبع عملية تنفيذ أوامر التطبيق خطوة بخطوة وتحديد مرحلة تشغيل التطبيق التي يحدث عنها الخطأ.

بعد أن يقوم المتخصصين في خدمة الدعم الفني بتحليل البيانات التي قمت بإرسالها، يمكنهم إنشاء برنامج AVZ النصي 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:

- 62 النظام حالة تقرير إنشاء
- 63 البيانات لفات إرسال
- 64 AVZ ل النصي البرنامج تنفيذ

إنشاء تقرير حالة النظام

➔ لإنشاء تقرير حالة النظام:

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 الزر أدوات الدعم. سيتم فتح النافذة أدوات الدعم.
 4. في النافذة التي ستفتح، انقر فوق الزر إنشاء تقرير حالة النظام.
- يتم إنشاء تقرير حالة النظام بالتنسيق HTML و XML ويتم حفظه في الأرشيف sysinfo.zip. عندما يتم تجميع المعلومات حول النظام، يمكنك عرض التقرير.

➔ لعرض تقرير:

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 الزر أدوات الدعم. سيتم فتح النافذة أدوات الدعم.

4. في النافذة التي ستفتح، انقر فوق الارتباط **عرض التقرير**.

سيتم فتح النافذة Microsoft Windows Explorer.

5. في النافذة التي ستفتح، قم بفتح لأرشيف المسمى sysinfo.zip الذي يحتوي على ملفات التقرير.

إرسال ملفات البيانات

بعد إنشاء ملفات التتبع وتقرير حالة النظام، فإنك بحاجة إلى إرسالها إلى خبراء الدعم الفني في Kaspersky Lab.

تحتاج إلى رقم طلب لتحميل الملفات إلى خدمة الدعم الفني (راجع القسم " Kaspersky حساب خبراء الدعم الفني على الحصول بي الخاص" على الصفحة 60). يوجد هذا الرقم في حسابي على Kaspersky على موقع خدمة الدعم الفني إذا كان طلبك فعالاً.

➤ **تحميل ملفات البيانات إلى خادم دعم 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 الزر **أدوات الدعم**.
سيتم فتح النافذة **أدوات الدعم**.
4. في النافذة التي سيتم فتحها، انقر فوق الزر **إرسال بيانات الخدمة إلى الدعم الفني**.
ومن ثم تفتح نافذة **إرسال تقرير**.
5. حدد خانة الاختيار الموجودة بجانب ملفات التتبع التي ترغب في إرسالها إلى خدمة الدعم الفني، ثم انقر فوق الزر **إرسال**.
تفتح النافذة **أدخل رقم الطلب**.
6. حدد الرقم الذي تم تحديده لطلبك من خلال الاتصال بخدمة الدعم الفني من خلال حسابي في Kaspersky، ثم انقر فوق الزر **الزر موافق**.

يتم حزم ملفات التتبع المحددة وإرسالها إلى خادم خدمة الدعم.

إذا كان من غير الممكن لأي سبب من الأسباب الاتصال بخدمة الدعم الفني، يمكن تخزين ملفات البيانات على جهاز الكمبيوتر وإرساله فيما بعد 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 الزر **أدوات الدعم**.
4. سيتم فتح النافذة **أدوات الدعم**.
5. في النافذة التي سيتم فتحها، انقر فوق الزر **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 الزر **إرسال**.

تفتح النافذة **أدخل رقم الطلب**.

7. انقر فوق الزر **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 خدمة الدعم الفني من حسابي في Kaspersky.

تنفيذ البرنامج النصي لـ AVZ

ننصح بعدم تغيير نص البرنامج النصي AVZ الذي استلمته من خبراء Kaspersky Lab. في حالة حدوث مشكلة أثناء تنفيذ البرنامج النصي، اتصل بخدمة الدعم الفني (راجع القسم "الفني الدعم على الإنترنت" في صفحة 60).

➔ 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 الزر **أدوات الدعم**.

سيتم فتح النافذة **أدوات الدعم**.

4. في النافذة التي ستفتح، انقر الزر **تشغيل البرنامج النصي**.

سيتم فتح النافذة **تنفيذ برنامج AVZ النصي**.

5. انسخ النص من البرنامج النصي المرسل بواسطة المتخصصين في خدمة الدعم الفني، وألصقه في حقل الإدخال في النافذة التي ستفتح وانقر فوق الزر **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 خطأ تتعلق بهذا الأمر.

المصطلحات

تنشيط التطبيق

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

رمز التنشيط

رمز تستلمه عند شراء الترخيص التجاري لـ Kaspersky Anti-Virus. وهو مطلوب لتنشيط التطبيق.

يعتبر رمز التنشيط عبارة عن سلسلة فريدة مكونة من عشرين حرف أبجدي رقمي في تنسيق xxxxx-xxxxx-xxxxx-xxxxx.

الوحدات النمطية للتطبيق

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

إعدادات التطبيق

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

الأرشيف

ملف واحد أو عدة ملفات تم حزمها في ملف واحد عن طريق الضغط. مطلوب ملف تطبيق أرشفة مخصص لحزم البيانات وفك حزمها.

التحديث المتاح

مجموعة تحديثات لوحدات تطبيق Kaspersky Lab تتضمن التحديثات الهامة المترجمة خلال فترة معينة من الزمن والتغييرات على بنية التطبيق.

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.

قاعدة بيانات عناوين الويب الخبيثة

قائمة بعناوين ويب التي تشتمل على محتوى يمكن اعتباره خطراً. وتم إنشاء هذه القائمة بواسطة أخصائيي Kaspersky Lab. ويتم تحديثها بصفة منتظمة ويتم تضمينها في حزمة تطبيق Kaspersky Lab.

قاعدة بيانات عناوين الويب الاحتمالية

قائمة بعناوين ويب، يتم تعريفها بعناوين احتمالية بواسطة خبراء Kaspersky Lab. يتم تحديث قاعدة البيانات بانتظام بالإضافة إلى جزء من تطبيق Kaspersky Lab.

قواعد البيانات

قواعد البيانات التي تحتوي على أوصاف لتهديدات الأمان الخاصة بالكمبيوتر والمعروفة لـ Kaspersky Lab منذ لحظة إصدار قاعدة 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.

حذف كائن

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

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.

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 المسؤول 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.

استثناء

الاستثناء عبارة عن كائن تم استثناءه من الفحص بواسطة تطبيق Kaspersky Lab. ويمكنك استثناء ملفات ذات تنسيق محدد من الفحص أو أفضة الملف أو منطقة محددة (على سبيل المثال مجلد أو برنامج) أو عمليات التطبيق أو كائنات حسب نوع التهديد وفقاً لتصنيف موسوعة الفيروسات. ويمكن تعيين مجموعة الاستثناءات لكل مهمة.

إنذار خاطئ

هو حالة يعتبر فيها تطبيق Kaspersky Lab أحد الكائنات غير المصابة على أنه كائن مصاب بسبب تشابه رمزه مع رمز أحد الفيروسات.

قناع الملف

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

المحلل المساعد على الاكتشاف

تقنية لاكتشاف معلومات التهديدات التي لم يتم إضافتها حتى الآن إلى قواعد بيانات Kaspersky Lab. يسمح المحلل المساعد على الاكتشاف باكتشاف الكائنات التي قد يسبب أداؤها في النظام تهديداً للأمان. 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).

تقنية ICHECKER

هي تقنية تزيد من سرعة عمليات الفحص لمكافحة الفيروسات من خلال استثناء الكائنات التي لم تتغير منذ آخر مرة تم فحصها، بشرط عدم تغير معلمات الفحص (إعدادات وقاعدة بيانات مكافحة الفيروسات). ويتم تخزين المعلومات الخاصة بكل ملف في قاعدة بيانات خاصة. ويتم استخدام هذه التقنية في كل من الحماية في الوقت الحقيقي وأوضاع الفحص عند الطلب.

على سبيل المثال، لديك ملف أرشيف تم فحصه بواسطة تطبيق Kaspersky Lab وتعيينه إلى الحالة غير مصاب. 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 مكافحة الفيروسات، سيتم 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 التكنولوجيا عدداً محدوداً من التنسيقات.

تطبيق غير متوافق

تطبيق مكافحة فيروسات من تطوير طرف ثالث أو تطبيق Kaspersky Lab لا يدعم الإدارة عبر برنامج Kaspersky Anti-Virus.

كائن قابل للإصابة

هو كائن، بالنظر لهيكله أو تنسيقه، يمكن للدخلاء استخدامه كـ "وعاء" لتخزين رمز خبيث وتوزيعه. وكقاعدة، تكون هذه الملفات قابلة للتنفيذ، على سبيل المثال يكون لها الملحق com، exe، dll، الخ. وتكون نسبة خطر تنشيط أي كود خبيث في مثل هذه الملفات كبيرة جداً.

كائن مصاب

كائن جزء من الرمز البرمجي الخاص به يكمل جزءاً من تهديد معروف. لا توصي Kaspersky Lab باستخدام مثل هذه الكائنات.

خوادم تحديث KASPERSKY LAB

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

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. يضمن استخدام البيانات من شبكة أمان Kaspersky زيادة وقت الاستجابة من تطبيقات Kaspersky Lab عند مواجهة أنواع جديدة من التهديدات، كما يعمل ذلك على تحسين فاعلية بعض مكونات الحماية والتقليل من خطر الحالات الإيجابية الخاطئة.

راصد لوحة المفاتيح

برنامج مصمم للتسجيل الخفي للمعلومات حول المفاتيح التي قام المستخدم بالضغط عليها. يطلق أيضاً على راصدات لوحة المفاتيح إما معترضي المفاتيح أو جواسيس المفاتيح.

مدة الترخيص

تعتبر فترة صلاحية الترخيص عبارة عن فترة زمنية يمكنك خلالها الوصول إلى ميزات التطبيق والحقوق الخاصة به لاستخدام الخدمات الإضافية.

حذف الرسائل

هي طريقة لمعالجة رسالة البريد الإلكتروني التي يتم خلالها حذف الرسالة مادياً. 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).

تطبيق على نمط مترو

تطبيق على الشاشة بأكملها يركز على المحتوى على حساب تبسيط عناصر الواجهة. تتميز التطبيقات من نمط Metro بمعلومات ذات بنية دقيقة، وتصميم موحد، ودعم التحكم الحساس للمس، والتكامل المتبادل.

ويتم دعم التطبيقات من نمط Metro في نظام التشغيل Microsoft Windows 8 فقط.

الاحتيال

نوع من نوع من التزوير عبر الإنترنت، عندما يتم إرسال رسائل البريد الإلكتروني بغرض سرقة المعلومات السرية. كقاعدة، تتعلق هذه المعلومات بالبيانات السرية.

كائن يُحتمل كونه مصابًا

كائن يحتوي الرمز الخاص به على رمز برمجي خبيث من تهديد أو رمز برمجي معروف، مشابه لأحد التهديدات أو الرموز البرمجية، ويتم الحكم عليه وفقًا لسلوكه.

بريد إلكتروني يُحتمل أن يكون غير مرغوب فيه

هي رسالة لا يمكن اعتبارها دون غموض بريدًا إلكترونيًا غير مرغوب فيه، لكنه تبدو عليها العديد من سمات رسائل البريد الإلكتروني غير المرغوب فيها (على سبيل المثال بعض أنواع المراسلات والرسائل الإعلانية).

مكونات الحماية

أجزاء لا تتجزأ من Kaspersky Anti-Virus تهدف إلى الحماية ضد أنواع محددة من التهديدات (على سبيل المثال، مكافحة البريد الإلكتروني غير المرغوب به أو مكافحة الاحتيال). يعتبر كل مكون من المكونات مستقلاً بشكل نسبي عن المكونات الأخرى ليكون من الممكن تعطيلها أو تكوينها بشكل مستقل.

البروتوكول

مجموعة من القواعد القياسية المعرفة بوضوح التي تنظم التعامل بين أي عميل وأي خادم. تعتبر بروتوكولات HTTP و FTP و NNTP إحدى البروتوكولات والخدمات التي تتعلق بها المعروفة.

الخادم الوكيل

خدمة شبكية لأجهزة الكمبيوتر تسمح للمستخدمين بتوجيه طلبات غير مباشرة إلى خدمات الشبكة الأخرى. أولاً، يقوم المستخدم بالاتصال بالخادم الوكيل ويطلب الحصول على مورد (ملف مثلاً) موجود على خادم آخر. ثم يقوم الخادم الوكيل بالاتصال بالخادم المحدد ويحصل على المورد منه، أو يقوم بإرجاع المورد من مخزنه المؤقت (في حالة إذا كان للخادم الوكيل مخزن مؤقت خاص به). وفي بعض الحالات، يمكن تعديل طلب المستخدم أو استجابة الخادم بواسطة الخادم الوكيل لأغراض معينة.

العزل

مخزن مخصص لوضع النسخ الاحتياطية لملفات التطبيق التي تم تعديلها أو حذفها أثناء التنظيف. يتم تخزين نسخ الملفات في تنسيق خا، حتى لا تمثل أي تهديد على الكمبيوتر.

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 متخف تماماً. بإمكان فيروس الجذر في الغالب أيضاً 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 الجذر تقوم بتنصيب برامج تشغيل وخدمات خاصة بها هي على نظام التشغيل (حيث تكون هذه الخدمات أيضاً "غير مرئية").

البرنامج النصي

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

مستوى الأمان

مستوى الأمان محدد كمجموعة محددة مسبقاً من الإعدادات لمكون التطبيق.

البريد الإلكتروني غير المرغوب فيه

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

كائنات بدء التشغيل

مجموعة البرامج اللازمة لبدء نظام التشغيل والبرامج المثبتة على جهاز الكمبيوتر وعملها بصورة صحيحة. يتم تنفيذ هذه الكائنات في كل مرة يبدأ فيها نظام التشغيل. توجد فيروسات قادرة على إصابة كائنات بشكل خاص، مما قد يؤدي على سبيل المثال إلى منع بدء تشغيل نظام التشغيل.

المهمة

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

إعدادات المهام

هي إعدادات التطبيق الخاصة بكل نوع من أنواع المهام.

مستوى التهديد

مؤشر يظهر احتمالية تشكيل تطبيق لخطر على نظام التشغيل. يتم حساب مستوى التهديد باستخدام التحليل المساعد على الاكتشاف وفقاً لنوعين من المعايير:

- ثابت (مثل معلومات حول الملف القابل للتنفيذ للتطبيق: الحجم وتاريخ الإنشاء وما إلى ذلك)؛
- معايير ديناميكية يتم استخدامها أثناء تحفيز تشغيل التطبيق في بيئة افتراضية (تحليل استدعاءات التطبيق لوظائف النظام).

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

التتبعات

تشغيل التطبيق في وضع التصحيح، وبعد أن يتم تنفيذ كل أمر، يتم إيقاف التطبيق، ويتم عرض نتيجة هذه الخطوة.

فحص الحركة

هو فحص في الزمن الحقيقي باستخدام معلومات (أحدث) إصدار حالي من قواعد البيانات للكائنات المنقولة عبر جميع البروتوكولات (مثل HTTP و FTP... إلخ)

العملية الموثوقة

هي أحد عمليات البرنامج التي لا يتم مراقبة عمليات الملف الخاص بها بواسطة تطبيق Kaspersky Lab في وضع الزمن الحقيقي. عند اكتشاف وجود نشاط مريب لعملية موثوق بها، يستبعد Kaspersky Anti-Virus العملية من قائمة العمليات الموثوق بها ويمنع جميع الأنشطة الخاصة بها.

فيروس غير معروف

هو فيروس جديد لا توجد عنه أية معلومات في قواعد البيانات. عادة يكتشف التطبيق الفيروسات غير المعروفة في الكائنات باستخدام المحلل المساعد، ويتم تصنيف تلك الكائنات على أنها كائنات يحتمل كونها مصابة.

التحديث

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

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.

فيروس

برنامج يصيب البرامج الأخرى عن طريق إضافة رمزه إليهم للحصول على التحكم عندما يتم تشغيل الملفات المصابة. ويسمح هذا التعريف البسيط بتعريض الإجراء الأساسي المنفذ من قبل أي عدوى فيروسية.

انتشار الفيروسات

سلسلة من المحاولات المتعددة لإصابة الكمبيوتر بفيروس.

قابلية الاختراق

عيب في نظام التشغيل أو التطبيق الذي يمكن أن يكون إما تطبيق مهدد للأمان من خلال صناع البرامج الخبيثة لاختراق النظام أو التطبيق وإتلاف تكامله. وجود عدد كبير من نقاط الضعف في النظام يجعل من الصعب الاعتماد عليه، لأن الفيروسات التي اخترقت النظام قد تتسبب في فشل التشغيل في النظام نفسه وفي التطبيقات المثبتة.

KASPERSKY LAB ZAO

يمتلك برنامج Kaspersky Lab شهرة كبيرة عالمية لحمايتها ضد الفيروسات والبرامج الضارة والبريد غير المرغوب فيه وهجمات الشبكة والمهاجمين 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 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 مقراً 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 الآسيوية. 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 الجواله الأخرى.

ويوفر Kaspersky Lab تطبيقات وخدمات لحماية محطات العمل والملفات وخواص 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 الموجهة لأجهزة الكمبيوتر. ولقد تم اعتماد منتجات Kaspersky Lab بواسطة كبرى معالم 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 جزءاً لا يتجزأ من أدوات مكافحة الفيروسات الحديثة من قبل Kaspersky Lab. وليست مصادفة استخدام مطورين آخرين لنواة نظام مكافحة فيروسات Kaspersky kernel في منتجاتهم، بما في ذلك: Safenet (الولايات المتحدة الأمريكية)، و Alt-N (الولايات المتحدة الأمريكية)، و Blue Coat Systems (الولايات المتحدة الأمريكية)، و Check Point Software Technologies (إسرائيل)، و Clearswift (المملكة المتحدة)، و CommuniGate Systems (الولايات المتحدة الأمريكية)، و Critical Path (أيرلندا)، و D-Link (تايوان)، و M86 Security (الولايات المتحدة الأمريكية)، و GFI (مالطا)، و IBM (الولايات المتحدة الأمريكية)، و Juniper Networks (الولايات المتحدة الأمريكية)، و LANDesk (الولايات المتحدة الأمريكية)، و Microsoft (الولايات المتحدة الأمريكية)، و NETASQ (فرنسا)، و NETGEAR (الولايات المتحدة الأمريكية)، و Parallels (روسيا)، و SonicWALL (الولايات المتحدة الأمريكية)، و WatchGuard Technologies (الولايات المتحدة الأمريكية)، و 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.

<http://www.kaspersky.com>

<http://www.securelist.com>

newvirus@kaspersky.com (مخصص فقط لإرسال الملفات محتملة الإصابة في تنسيق الأرشيف)

<http://support.kaspersky.com/virlab/helpdesk.html>

(للاستعلامات الموجهة إلى محلي الفيروسات)

<http://forum.kaspersky.com>

موقع ويب Kaspersky Lab:

موسوعة الفيروسات:

مختبر مكافحة الفيروسات:

منتدى ويب لـ Kaspersky Lab:

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يتم تضمين المعلومات الخاصة بالطرف الخارجي في الملف legal_notices.txt الموجود 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 و Pentium علامات تجارية لشركة Intel Corporation مسجلة في الولايات المتحدة الأمريكية وأي مكان آخر.

يعتبر كل من Microsoft و Windows و Windows Vista و Internet Explorer علامات تجارية لشركة Microsoft Corporation ومسجلة في الولايات المتحدة الأمريكية وأي مكان آخر.

يعتبر كل من Mozilla و Firefox علامات تجارية لشركة Mozilla.

KASPERSKY.....	72
KASPERSKY LAB.....	72
النهائي المستخدم ترخيص اتفاقية	24
المفاتيح لوحة اعتراض أجهزة	
الظاهرية المفاتيح لوحة	42
ذكية أداة	54
الذكية Kaspersky أدوات	54
إضافية أدوات	
وإصلاحها Microsoft Windows أخطاء استكشاف	36
الإنقاذ قرص	47
الخصوصية منظم	43
التطبيق إزالة	22
الاقتراضية الإعدادات استعادة	52
وإصلاحها Microsoft Windows أخطاء استكشاف	36
الإحصائيات	51
الإخطارات	30
النتبغات	
النتبع نتائج تحميل	63
التحديث	32
الترخيص	24
النهائي المستخدم ترخيص اتفاقية	24
التنشيط رمز	25
التشخيصات	31
التقارير	51
العزل	
كائن استعادة	35
المفتاح	24
سرية بيانات	40
التطبيق تثبيت	15
الأمان تحليل	31
الإعدادات استيراد / تصدير	54
التطبيق إلى الوصول تقييد	50
التطبيق تنشيط	29
تجريبي إصدار	18, 58
الترخيص	24
التنشيط رمز	25
الأمان تهديدات	31
الحماية حالة	31
التنشيط رمز	25
الحدث سجل	51
Kaspersky أمن شبكة	56

الإحصائيات عرض	51
الأمنية الثغرات فحص	39
الاختراق قابلية	39
الإنفاذ قرص	47
التطبيق بيانات قواعد	32
تنظيفه تم كائن	35
الظاهرية المفاتيح لوحة	42
الأجهزة متطلبات	13
البرامج متطلبات	13
الويب مواقع لعناوين Kaspersky مستشار	
الويب فيروسات مكافحة	46
الأمان مشكلات	31
التحديث مصدر	32
الاحتيال مكافحة	41
البريد فيروسات مكافحة	38
الويب فيروسات مكافحة	
أمن تصفح	46
الويب مواقع لعناوين Kaspersky مستشار	46
التطبيق مكونات	12
الألعاب بيانات ملف	47
الشاشة ملء في التطبيق تشغيل وضع	47