Kaspersky Internet Security 2013

Manual do Revisor

Sumário

Este guia explica como usar o Kaspersky Internet Security 2013 (KIS 2013), um produto integrado que oferece proteção aos sistemas Microsoft Windows XP, Vista e Windows 7 contra malware, cavalos de Troia, ataques de hackers, spam, spyware, phishing, vazamento de dados confidenciais e conteúdo indesejado.

1 Introdução

O Kaspersky Internet Security 2013 oferece proteção premium para PCs contra todas as ameaças da Internet, garantindo que você esteja sempre seguro enquanto usa a Web para transações bancárias, fazer compras, navegar, redes sociais e outros. Tecnologias exclusivas, como o Safe Money e o Teclado Seguro, protegem suas transações financeiras em bancos on-line, sistemas de pagamento como o PayPal e lojas virtuais. E nossa nova Prevenção Automática contra Explorações garante que vulnerabilidades não comprometam seu computador. Além disso, o Kaspersky Internet Security 2013 é otimizado para desempenho máximo, para que você não fique lento ao usar todo o potencial da Internet.

2 Principais benefícios

2.1 Proteção em tempo real contra todas as ameaças da Internet

A Internet nos oferece uma liberdade e uma conveniência enormes para comprar, usar o banco, acompanhar os amigos, baixar música, compartilhar imagens, etc., a qualquer hora do dia ou da noite e de quase qualquer lugar. Mas ela também pode nos deixar vulneráveis a vírus e outras ameaças da Internet que surgem continuamente, com uma taxa aproximada de 125.000 novos malwares por dia. Nossa inovadora **abordagem híbrida** de proteção combina a eficiência em tempo real da nuvem com as avançadas tecnologias de segurança de seu computador para dar uma resposta mais rápida e eficiente às atuais ameaças complexas e em constante evolução.

O KIS 2013 inclui um conjunto de tecnologias novas e atualizadas para oferecer proteção total ao seu computador durante todos os tipos de atividade on-line. Os exemplos incluem: nova tecnologia **Safe Money** para proteger dados pessoais durante transações financeiras; novo modo **Teclado Seguro** para proteger dados inseridos no teclado físico; **Proteção antiphishing** atualizada para manter seus dados pessoais a salvo de hackers e **Consultor de URLs**, que o adverte sobre o nível de perigo dos links da Web.

Você pode ler mais sobre segurança de Internet neste artigo:
Internet fraud for dummies: practical advice for protecting yourself against online scams (Fraude da Internet para iniciantes: conselhos práticos para se proteger contra golpes online
http://www.securelist.com/en/analysis/204792149/Internet_fraud_for_dummies_practical_advice_for_protecting_yourself_against_online_scams

2.2 Garante que vulnerabilidades não comprometam seu PC

Uma das maneiras mais fáceis pelas quais os criminosos virtuais encontram brechas na proteção dos usuários é através de vulnerabilidades de aplicativos e do sistema que não foram atualizados com as correções mais recentes. Por exemplo, programas populares, como Adobe Reader, Internet Explorer e Firefox, podem fornecer uma entrada fácil para programas maliciosos. O Kaspersky Internet Security 2013 inclui a nova **Prevenção Automática contra Explorações**, que vai além de simplesmente verificar vulnerabilidades; ela analisa e controla as ações de programas e aplicativos para que eles não possam causar danos.

Saiba mais neste whitepaper

2.3 Transações bancárias e compras on-line seguras

O Kaspersky Internet Security 2013 fornece camadas adicionais de proteção durante transações financeiras, como ao usar o banco on-line, sistemas de pagamento (por exemplo, o PayPal) e ao fazer compras em sites de comércio eletrônico. Nossa exclusiva tecnologia **Safe Money** garante que o site é seguro e que você não está sendo enganado por um site falso ou de phishing. E ela se oferece para abrir o site em um modo protegido especial, mantendo seu número de cartão de crédito e outros dados pessoais a salvo de ladrões virtuais.

Nosso novo **Teclado Seguro** é ativado automaticamente quando você abre um site de banco ou de pagamento, ou insere uma senha em qualquer página da Web, protegendo todas as informações inseridas em um teclado físico dos keyloggers. E, para a proteção completa de informações pessoais ao usar o banco on-line, implementamos o acesso rápido ao **Teclado Virtual** nos navegadores da Web. O **Teclado Virtual** permite usar cliques do mouse para inserir informações bancárias, de forma que elas não possam ser rastreadas ou roubadas por keyloggers, hackers ou ladrões de identidades.

Saiba mais neste whitepaper

2.4 Proteção proativa contra ameaças desconhecidas

Hoje em dia, novos malwares aparecem com uma velocidade incrível. Atualmente, cerca de 125.000 novas amostras a cada dia. Isso significa que a análise de assinaturas tradicionais sozinha não é mais suficiente para combatê-los de maneira eficiente. Por isso, a proteção proativa tornou-se um meio de defesa principal, analisando o comportamento de aplicativos e bloqueando-os, se parecerem suspeitos.

O KIS 2013 inclui o **Inspetor do Sistema**, que monitora e registra a atividade de todos os aplicativos no sistema, analisa seu comportamento e bloqueia todas as ações indesejadas. O Inspetor do Sistema também permite reverter as ações de qualquer malware.

Você pode ler mais sobre ameaças desconhecidas neste artigo:
Cybercrime Outlook 2020 from Kaspersky Lab (Panorama do crime virtual para 2020 pela Kaspersky Lab)
http://www.securelist.com/en/analysis/204792089/Browsing_malicious_websites

2.5 No caminho para a proteção em 'nuvem'

O cenário da segurança de software está mudando em uma velocidade cada vez maior, e o fato de dezenas de milhares de novos crimes virtuais aparecerem todos os dias significa que as regras para uma segurança de software eficiente mudaram. A fim de reagir rapidamente às novas ameaças, o KIS 2013, assim como a versão anterior, inclui o **Kaspersky Security Network**, um sistema de bancos de dados on-line nos servidores da Kaspersky Lab que contém informações sobre aplicativos confiáveis, perigosos e suspeitos. As informações na nuvem são atualizadas muito rapidamente e então disponibilizadas a todos os usuários de produtos da Kaspersky Lab. Cada vez que o usuário executa um arquivo no computador, o KIS consulta na nuvem as informações atualizadas sobre o aplicativo e seus direitos no sistema.

O KIS 2013 inclui recursos aprimorados para oferecer proteção em nuvem abrangente. A funcionalidade **Consultor de Arquivos** permite descobrir a reputação de arquivos possivelmente perigosos com um único clique do mouse. O **Consultor de URLs** informa sobre links para sites suspeitos ou perigosos, acessando na nuvem as informações mais recentes sobre os recursos on-line.

2.6 Proteção de sua identidade e sua privacidade digital

Sua identidade digital é protegida até mesmo das mais ardilosas fraudes on-line, com as mais recentes tecnologias antiphishing proativas e baseadas em nuvem. Além disso, o Kaspersky Internet Security 2013 oferece duas tecnologias de proteção exclusivas para inserir informações pessoais on-line. Nosso novo **Teclado Seguro** é ativado automaticamente quando você abre um site de banco ou de pagamento, ou insere uma senha em qualquer página da Web, protegendo todas as informações inseridas em um teclado físico dos keyloggers. E, para a proteção completa de suas informações pessoais ao usar o banco on-line, implementamos o acesso rápido ao **Teclado Virtual** nos navegadores da Web. O **Teclado Virtual** permite usar cliques do mouse para inserir informações bancárias, de forma que elas não possam ser rastreadas ou roubadas por keyloggers, hackers ou ladrões de identidades. O **Teclado Virtual** também pode ser executado a qualquer momento na interface principal do software.

2.7 Proteção de e-mails e mensagens instantâneas

O KIS 2013 oferece proteção de e-mails e mensagens instantâneas (ICQ, MSN, etc.). O **Antivírus de Email** verifica os e-mails enviados e recebidos no computador e bloqueia o conteúdo nocivo. Assim, você pode se comunicar sem se preocupar com ameaças e links suspeitos.

Você pode ler mais sobre ameaças de redes sociais neste artigo:
The Dangers of Social Networking (Os perigos das redes sociais)
http://www.securelist.com/en/analysis/204792113/The_Dangers_of_Soci33al_Networking

2.8 Proteção antispam usando informações da nuvem

O módulo **Antispam** pode reduzir significativamente o número de e-mails indesejados que você recebe. O **Antispam** é incorporado no cliente de email instalado no computador e verifica todas as mensagens recebidas. Os filtros analisam os cabeçalhos e o conteúdo das mensagens, além de todas as imagens anexadas. O mecanismo **Antispam** atualizado do KIS 2013 utiliza as mais recentes tecnologias em nuvem e usa a detecção proativa, o que aumenta significativamente a eficiência do reconhecimento de spam. Além disso, o módulo **Antispam** não requer um treinamento, pois ele tem acesso ao banco de dados em nuvem de exemplos de mensagens de spam.

2.9 Controle para Pais avançado

O **Controle para Pais** foi criado para proteger as crianças de ameaças no computador e na Internet. O KIS 2013 oferece uma grande variedade de funções relacionadas. É possível controlar o acesso ao computador e à Internet, quais aplicativos podem ser executados, limitar os downloads de arquivos da Internet e controlar o acesso a redes sociais e contatos. Além disso, essa função pode ser usada para ver relatórios estatísticos das ações dos usuários controlados.

Você pode ler mais sobre o Controle para Pais neste artigo:
Parental Control and the Internet (Controle para Pais e a Internet)
http://www.securelist.com/en/analysis/204792143/Parental_Control_and_The_Internet

2.10 Proteção sem dificuldades com máximo desempenho do computador

Nossa meta pessoal é fornecer a você a proteção definitiva sem comprometer o desempenho do sistema ou incomodá-lo com perguntas e alertas. Otimizado para o desempenho máximo do computador durante seu uso ativo diário, o Kaspersky Internet Security 2013 trabalha em segundo plano, verificando a reputação de todos os aplicativos e sites executados, analisando o comportamento dos programas, atualizando seus bancos de dados e muito mais, para garantir que você esteja sempre seguro. Tudo isso, sem tornar o computador lento.

2.11 Rescue Disk

O **Rescue Disk** é um disco de inicialização que contém um conjunto de recursos para detectar e neutralizar infecções no computador quando não é possível carregar normalmente o sistema operacional e o software antivírus. É possível usar CD de instalação com essa finalidade (se a caixa foi comprada em uma loja), o que é muito conveniente quando não há um segundo computador para baixar um disco de recuperação da Internet.

3 Instalação e Ativação

O KIS 2013 otimiza de maneira significativa o processo de instalação do produto, automatizando grande parte da instalação e reduzindo significativamente o número de etapas executadas manualmente. Um instalador Web especial foi integrado diretamente no produto. Quando o usuário baixa e executa o produto no site, ele verifica automaticamente a versão mais recente do produto, inicia o download e a instalação, remove software incompatível e executa a desinfecção, caso algo tente impedir a instalação do produto.

3.1 Requisitos de sistema

O KIS 2013 é otimizado para usar uma quantidade mínima de recursos do sistema. Isso inclui:

- Sistema operacional: Microsoft Windows 7, Windows Vista ou Windows XP (32 ou 64 bits).
- Processador: CPU de 800 MHz para Windows XP ou CPU de 1 GHz para Windows Vista ou Windows 7
- RAM: 512 MB para Windows XP ou 1 GB (32 bits)/2 GB (64 bits) para Windows Vista ou Windows 7
- Espaço em disco: 480 MB de espaço disponível no disco rígido para instalação

O KIS 2013 também requer uma unidade de CD (se o aplicativo foi comprado em CD), conexão com a Internet e o Internet Explorer 8 ou superiores (para a ativação do produto e atualizações do banco de dados).

Há uma lista completa de requisitos de sistema disponível em www.kaspersky.com ou no Manual do Usuário.

3.2 Instalação

Para iniciar a instalação do Kaspersky Internet Security 2013 no computador, execute o arquivo de instalação (com a extensão .EXE) no CD do produto. Antes da instalação, o programa verifica nos servidores de atualização da Kaspersky Lab se há uma versão mais recente do Kaspersky Internet Security. Se uma versão mais nova do produto estiver disponível, você terá a opção de baixá-la e instalá-la no seu computador.

O Kaspersky Internet Security 2013 é instalado usando o **Assistente de Instalação** interativo. O Assistente consiste em uma série de telas (etapas) pelas quais você pode navegar usando os botões Voltar e Avançar.

Instalação em um sistema operacional infectado

Às vezes, um computador pode estar infectado de tal forma que é impossível instalar uma solução antivírus, especialmente após a infecção por alguns tipos de rootkits. Nesse caso, o produto baixa um utilitário exclusivo automaticamente e neutraliza as infecções ativas no sistema antes de concluir o processo de instalação.

Kaspersky Security Network

Como parte do processo de instalação, o usuário é convidado a ingressar no **Kaspersky Security Network** (KSN). O KSN coleta e encaminha automaticamente à Kaspersky Lab informações sobre tentativas de infectar seu computador e os arquivos suspeitos detectados nele (em total anonimato e apenas com o consentimento do usuário). Essas informações são enviadas à Kaspersky Lab para análise e adicionadas ao nosso banco de dados on-line de malware. O KSN fornece o mais alto nível de detecção rápida de ameaças.

3.3 Ativação e configuração

Após a conclusão das funções do **Assistente de Instalação,** o **Assistente de Ativação** solicitará que você ative o programa. Nesse momento, você deverá inserir o código de ativação do produto. Os usuários que têm um código de ativação do KIS 2012 válido poderão usá-lo para ativar o KIS 2013. É necessária uma conexão com a Internet para ativar o aplicativo. Não é necessário reiniciar o computador após a instalação. Se o produto foi comprado pela Internet, agora a ativação é executada automaticamente, sem a necessidade de inserir o código de ativação. O código de ativação é adicionado automaticamente ao KAV/KIS 2013 durante o download do produto, usando o link contido no e-mail de compra.

A Kaspersky Lab recomenda executar uma verificação completa do disco rígido e de todos os dispositivos de armazenamento externos conectados ao computador imediatamente após a instalação. A duração da primeira verificação depende da velocidade da CPU e do número de arquivos no computador.

4 Visão Geral da interface

4.1 Janela principal

Informações comuns

A interface do KIS 2013 foi atualizada para torná-la mais amigável. A seção central exibe informações sobre o número de ameaças detectadas, o status de atualização dos bancos de dados de antivírus e o período de licença restante antes da expiração.

Proteção em nuvem

Ao clicar em **Proteção em nuvem,** você recebe informações detalhadas sobre as tecnologias em nuvem integradas ao KIS 2013 e poderá avaliar sua eficiência.

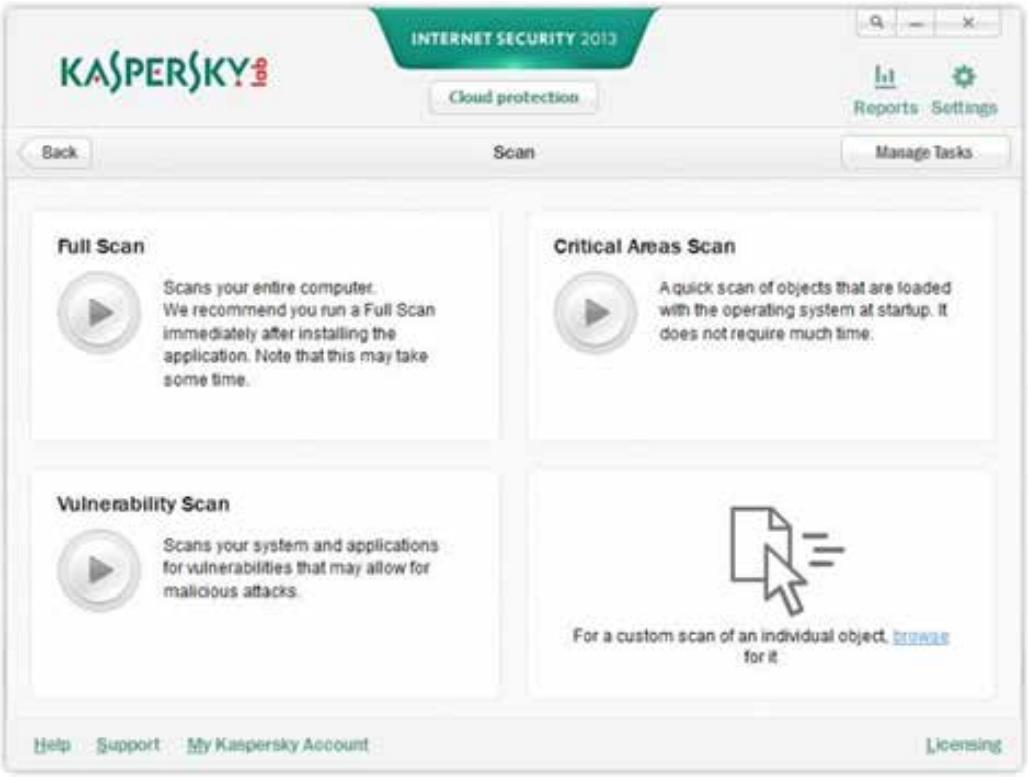
Componentes do programa

A parte inferior da janela principal exibe os principais componentes do produto. Ao clicar no ícone com o símbolo de seta, você abre a lista completa de componentes do produto:

4.2 Verificação

A verificação do computador quanto à presença de vírus e vulnerabilidades é um dos elementos mais importantes da segurança. É essencial executar verificações periódicas do computador para eliminar a disseminação de qualquer malware que não tenha sido detectado pelos componentes de proteção devido, por exemplo, ao baixo nível de uma configuração de segurança personalizada.

Para verificar se há malware no computador, é recomendável executar uma **Verificação Completa** ou uma **Verificação de Áreas Críticas.** A **Verificação de Áreas Críticas** abrange os objetos que são carregados com o sistema operacional, a memória do sistema, os setores de inicialização do disco rígido e outros objetos que você adicionar.



Essa guia também pode ser usada para executar a verificação de pastas ou arquivos específicos

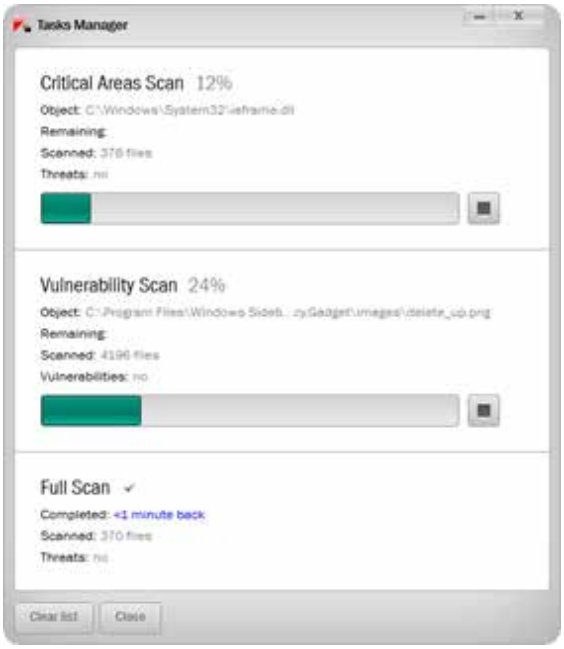
Verificação de Vulnerabilidades

As vulnerabilidades no sistema operacional podem ser resultantes de falhas de software ou design, senhas não confiáveis, ataques maliciosos, etc. As vulnerabilidades são encontradas examinando o sistema, procurando anomalias ou corrupções nas configurações do sistema operacional, pesquisando serviços vulneráveis e outras medidas de segurança.

A **Verificação de Vulnerabilidades** abrange todos os aplicativos instalados no computador do usuário e compara cada um deles com os maiores bancos de dados de vulnerabilidades conhecidas do mundo, criados e gerenciados pela Secunia, uma empresa dinamarquesa especializada no fornecimento de informações sobre vulnerabilidades críticas de software em diversos sistemas operacionais.

Gerenciar tarefas

O KIS 2013 permite exibir as tarefas executadas pelo aplicativo e revisar seu status. Assim, é possível otimizar os recursos do computador.



4.3 Atualização

A atualização dos bancos de dados e módulos do Kaspersky Internet Security 2013 mantém seu computador seguro contra as ameaças mais recentes. Todos os dias, vemos aparecerem novos vírus, cavalos de Troia e outros malwares. Os bancos de dados do Kaspersky Internet Security 2013 contêm informações sobre ameaças e formas de neutralizá-las. Portanto, o aplicativo e seus bancos de dados de antivírus devem ser atualizados para proteger seu computador contra novas ameaças. O KIS 2013 é atualizado automaticamente, mas você pode baixar atualizações na guia **Atualização**, se necessário.

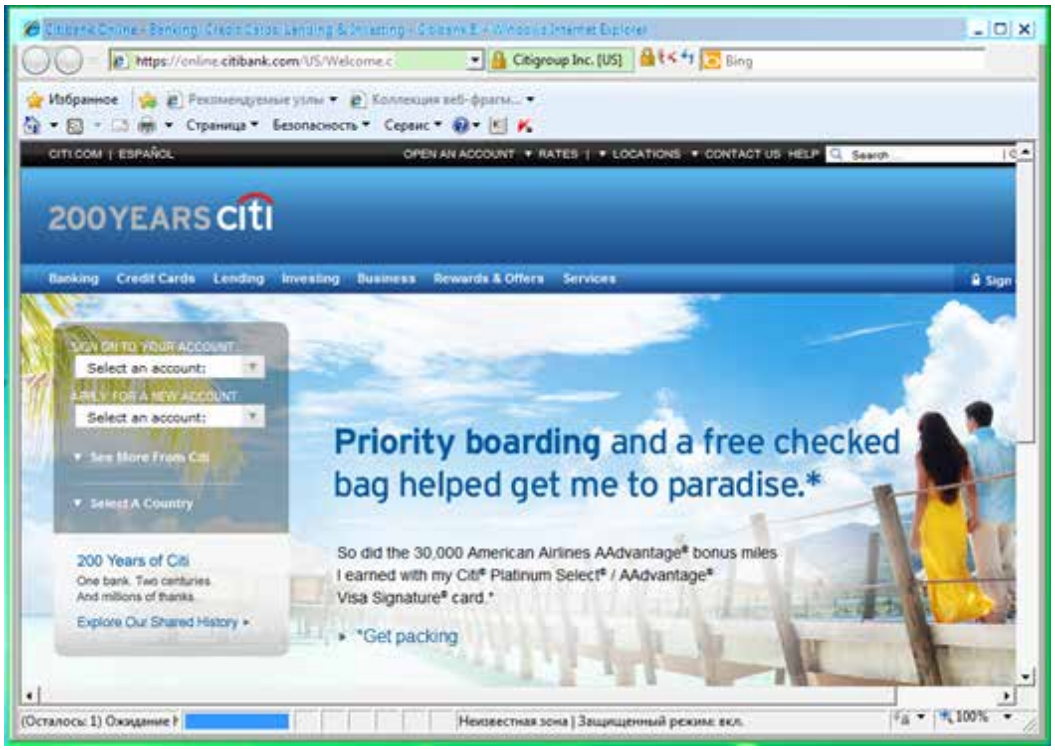
4.4 Safe Money – Novo!

Para proteger os dados confidenciais que você insere em sites de bancos e sistemas de pagamento (como números de cartões bancários, senhas de acesso a serviços de bancos on-line), além de impedir o roubo de ativos ao fazer pagamentos on-line, o Kaspersky Internet Security 2013 inclui a exclusiva tecnologia **Safe Money**.

Como ela funciona.

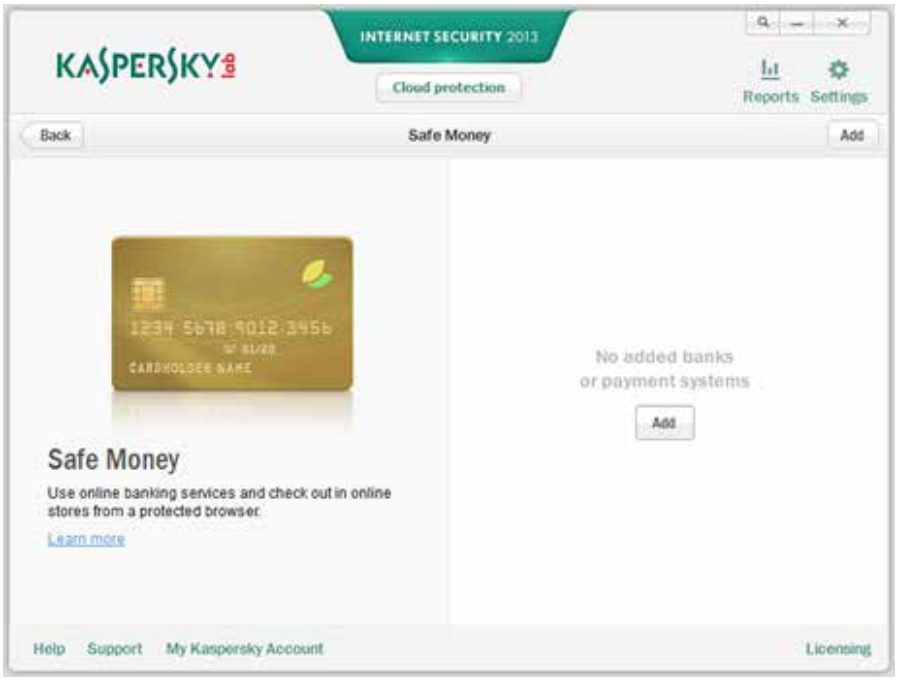
O produto:

- Verifica se a solicitação vai para o site original do banco ou sistema de pagamento (em relação a uma lista atualizável de sites do produto).
- Verifica o certificado de segurança para evitar o redirecionamento para um site falso.
- Verifica vulnerabilidades críticas de bancos on-line no sistema operacional.
- Se oferece para abrir o site no modo **Safe Money** para proteger seus dados pessoais contra roubo. Nesse caso, o KIS 2013 restringe o acesso de outros programas e processos aos dados transferidos no modo **Safe Money**, o que ajuda a garantir a proteção de seus dados pessoais contra roubo. Quando o modo **Safe Money** está ativado, aparece um quadro verde ao redor da janela do navegador.



Quando a transação de pagamento via **Safe Money** é concluída, o usuário é redirecionado automaticamente para uma janela normal do navegador a fim de terminar o processo ou continuar a compra na loja virtual.

Para adicionar sites de bancos, pagamento ou compras, escolha **Safe Money** na parte inferior da janela e clique no link Adicionar.



Para abrir as configurações detalhadas desse recurso, clique no link **Configurações** na parte superior da janela principal e selecione **Safe Money** na lista de componentes do produto.

Ao mesmo tempo, para evitar que os dados confidenciais inseridos usando um teclado sejam interceptados, há duas opções disponíveis:

- **O Teclado Virtual,** exibido na tela do usuário e controlado pelo mouse.
- **O Teclado Seguro**, um novo recurso que usa um driver especial para proteger dados inseridos em um teclado físico.

(As duas tecnologias são descritas detalhadamente a seguir).

4.5 Controle para Pais

O **Controle para Pais** foi criado para proteger as crianças de ameaças no computador e na Internet. Ele permite impor diferentes tipos de restrições:

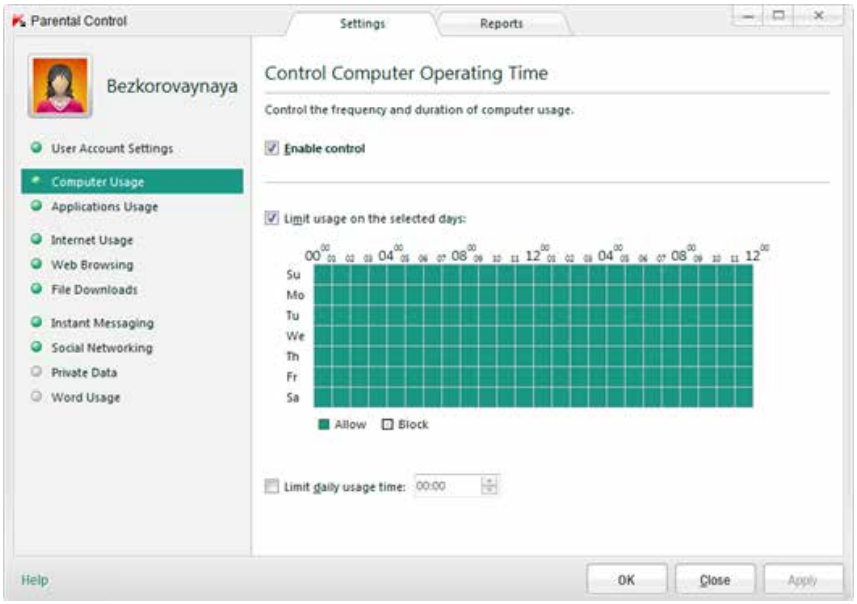
1. Limitar o tempo de operação do computador.
2. Bloquear ou permitir o acesso a aplicativos específicos no computador.
3. Bloquear ou permitir o acesso a sites específicos.
4. Controlar o uso de e-mail, mensagens instantâneas (ICQ, MSN) e redes sociais (Facebook, etc.) por seus filhos. Uma lista completa de serviços de mensagens instantâneas e redes sociais é fornecida a seguir.
5. Controlar downloads de arquivos.
6. Controlar a transferência de informações pessoais.

O **Controle para Pais** dá suporte aos seguintes serviços de mensagens instantâneas: ICQ, QIP. MSN, Yahoo Messenger, Google Talk, mIRC, Mail.RU Agent, Psi, Miranda, AIM. Digsby, Pidgin, Qnext, SIM, Trilian, Xchat, Instantbird, RnQ, Jabber.

E às seguintes redes sociais: MySpace, Twitter, Facebook.

Controlar o tempo de operação do computador

Você pode usar o **Controle para Pais** para limitar o tempo que o computador é usado. É possível programar o tempo de acesso de seus filhos ao computador (dias da semana e horário durante o dia), além de limitar o tempo por dia que o computador fica em uso.



Controle de Redes Sociais

O Controle de Redes Sociais permite controlar os contatos de seus filhos em redes sociais. Você pode bloquear os contatos indesejados e controlar o conteúdo das mensagens enviadas e recebidas. Também é possível criar listas de contatos permitidos e bloqueados, definir palavras-chave e frases que serão verificadas nas mensagens, além de especificar informações pessoais que não podem ser enviadas

4.6 Atividade de aplicativos

Para exibir a lista de aplicativos executados em seu computador e processos em execução, abra a janela principal do aplicativo e selecione a seção **Atividade de Aplicativos** na parte inferior.

4.7 Monitor de Rede

O Monitor de Rede é uma ferramenta usada para exibir informações sobre atividades de rede em tempo real. Para exibir informações sobre atividades de rede, abra a janela principal do aplicativo e selecione a seção **Atividade de Rede** na parte inferior.

4.8 Teclado Virtual e Teclado Seguro

Teclado Virtual – Aprimorado!

O **Teclado Virtual** impede a interceptação de pressionamentos de teclas por spyware de teclado (keyloggers) e a transferência de informações bancárias pessoais e outras informações confidenciais para os criminosos virtuais. Como em um teclado normal, você pode usar o **Teclado Virtual** para inserir qualquer texto; basta pressionar os botões correspondentes com a seta do mouse. A tecnologia inserida fornece proteção confiável contra a mais recente geração de aplicativos capazes de capturar imagens da tela e contra vazamentos de dados pelos navegadores da Web.

No KIS 2013, abrir o **Teclado Virtual** é ainda mais fácil e conveniente. Quando são abertos sites de bancos ou de pagamento no navegador da Web, o elemento de início rápido do **Teclado Virtual** é ativado automaticamente no campo de entrada.

Teclado Seguro – Novo!

O KIS 2013 inclui um novo recurso para a proteção adicional de dados pessoais ao usar um teclado físico. Se você abre um site de banco ou pagamento, ou insere uma senha em qualquer página da Web, o **Teclado Seguro** é ativado automaticamente. As configurações do produto permitem selecionar outras categorias de sites em que o modo de proteção **Teclado Seguro** deve ser ativado.

Teclado Virtual x Teclado Seguro

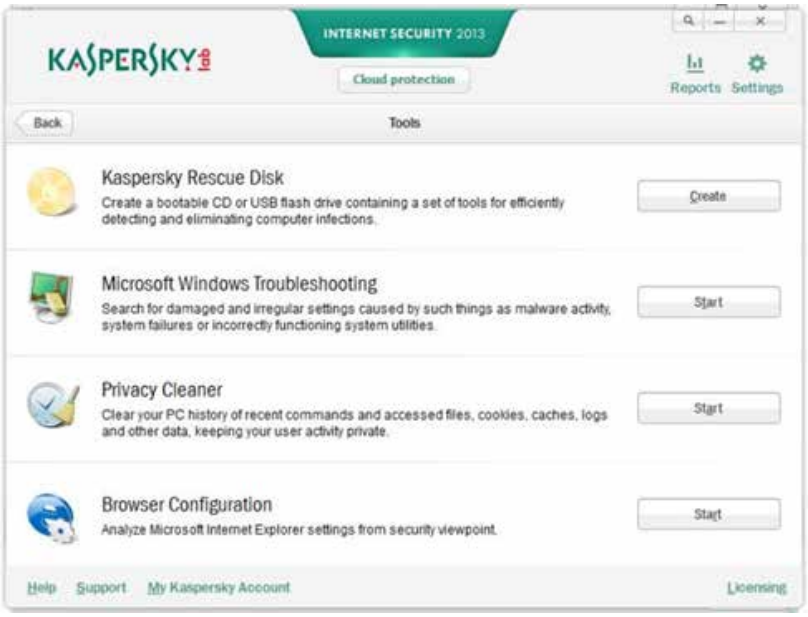
O **Teclado Virtual** o protege de uma grande variedade de ameaças, e recomendamos usá-lo em transações financeiras sigilosas. No entanto, como ele precisa ser iniciado manualmente, também criamos a tecnologia **Teclado Seguro** para proteger a entrada no teclado em todos os momentos.

4.9 Quarentena

A quarentena é uma área de armazenamento especial para arquivos com grande probabilidade de infecção por vírus e arquivos que não podem ser desinfetados logo que são detectados. Eles são armazenados em um formato especial e não representam um perigo para o sistema. Os arquivos colocados na quarentena são verificados sempre que os bancos de dados de antivírus são atualizados.

4.10 Ferramentas

A guia Ferramentas contém um conjunto de ferramentas adicionais que fornecem mais proteção para o computador.



Rescue Disk Kaspersky

Determinados malwares causam danos aos arquivos necessários para iniciar o sistema operacional. Quando isso ocorre, você pode usar o **Rescue Disk**. Trata-se de um disco de inicialização que contém um conjunto de ferramentas para detectar e neutralizar infecções no computador quando não é possível carregar normalmente o sistema operacional e o software antivírus.

O KIS 2013 oferece a opção de usar o disco de distribuição do produto (se a caixa com o produto foi comprada em uma loja) como disco de recuperação. Para fazer isso, insira o disco de distribuição do produto na unidade de CD/DVD e, no BIOS, selecione a opção de inicialização CD/DVD. Assim, você não precisa mais fazer um disco de recuperação antecipadamente ou usar outro computador para criá-lo.

Solução de problemas do Microsoft Windows

Este assistente pode ajudar a restaurar o sistema operacional Windows depois que ele travar ou for danificado devido a um ataque malicioso. Nossos especialistas recomendam desativar a função de inicialização automática usando a memória flash, a fim de aumentar a segurança.

Configurações do navegador

O assistente de configurações do navegador analisa detalhadamente as configurações do Internet Explorer e sugere maneiras de aprimorá-las com base nas recomendações da Kaspersky Lab. Com seu consentimento, essas configurações podem ser alteradas para melhorar a segurança e a proteção de suas informações confidenciais ao trabalhar no Internet Explorer. Essas alterações podem incluir, por exemplo, o bloqueio de componentes ActiveX ou a exclusão de arquivos com informações confidenciais da memória cache.

Eliminação de rastros de atividades

Os usuários sempre deixam rastros de suas atividades, como dados inseridos em fóruns da Web, informações sobre os sites visitados ou os nomes de arquivos e pastas salvos no computador.

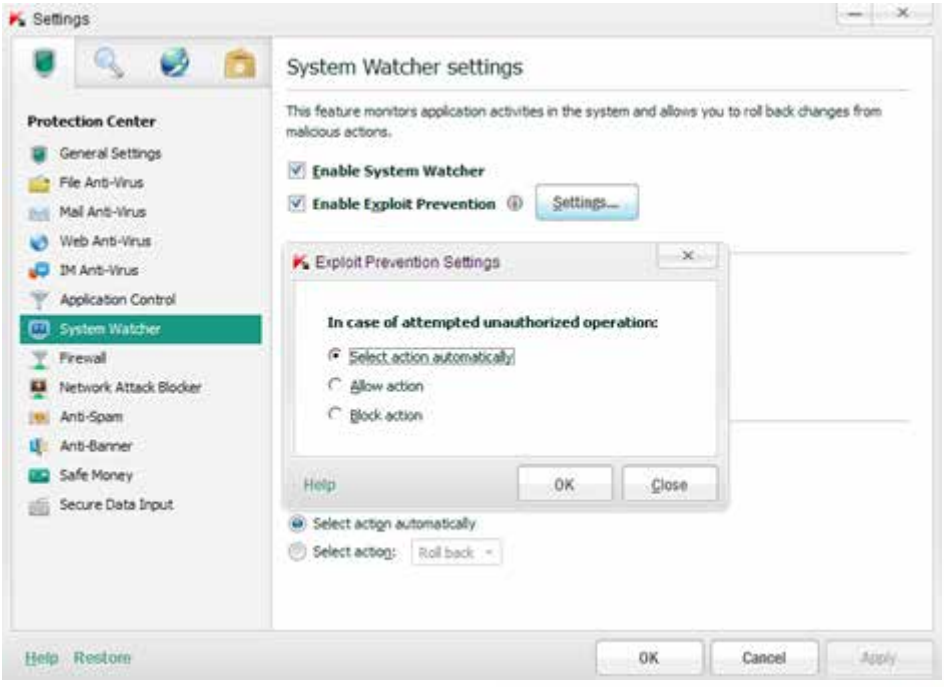
Para garantir a confidencialidade do usuário, é recomendável excluir essas informações. Isso é essencial, por exemplo, quando o computador é usado por mais de uma pessoa. As informações também podem ser roubadas através de uma rede.

4.11 Prevenção Automática contra Explorações – Novo!

É comum que programas maliciosos explorem vulnerabilidades em aplicativos populares, como Adobe Reader, Internet Explorer e Firefox, para tentar obter o controle do computador, roubar seus dados pessoais, etc. **O KIS 2013 inclui uma nova tecnologia, a Prevenção Automática contra Explorações, que impede e bloqueia essas explorações**. Suas características incluem:

1. Controle sobre a inicialização de arquivos executáveis (inclusive navegadores da Web), caso sejam encontradas vulnerabilidades, ou de aplicativos que não se destinam à inicialização de arquivos executáveis (Microsoft Word, Excel, etc.).
2. Se forem iniciados arquivos executáveis, são verificados sinais de comportamento de explorações em suas atividades.
3. Controle de todas as atividades executadas por um aplicativo no qual foi detectada uma vulnerabilidade (por exemplo, seguir um link, gravar outros processos na memória, etc.). Para garantir a proteção mais eficiente, todas as informações (como a lista de aplicativos com vulnerabilidades detectadas, o controle sobre a inicialização de arquivos executáveis por aplicativos) podem ser atualizadas.

As configurações estão disponíveis na janela de configurações do **Inspetor do Sistema:**



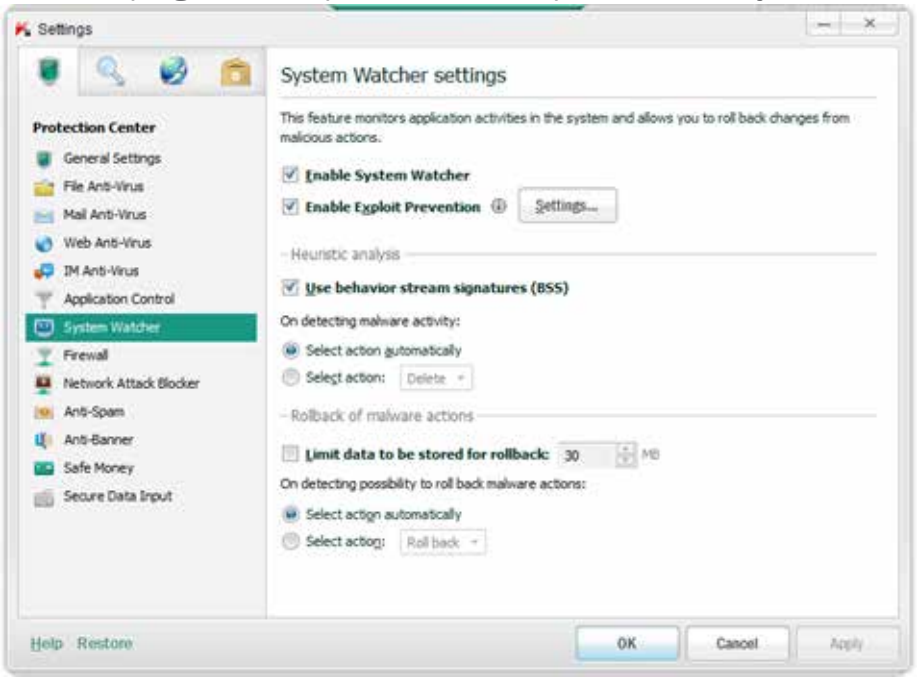
4.12 Inspetor do Sistema

O KIS 2013 inclui o **Inspetor do Sistema**, uma nova tecnologia que monitora todas as ações realizadas pelos programas em execução no computador e compara o comportamento de cada programa com padrões de comportamentos de malware. Isso identifica de maneira eficiente programas novos, suspeitos e perigosos.

O **Inspetor do Sistema** também permite reverter alterações de malware.

Quando são usadas tecnologias proativas, é muito importante poder reverter as ações executadas pelos programas, se eles forem considerados maliciosos. O KIS 2013 oferece essa função. Dependendo das configurações do produto, a reversão de ações maliciosas é executada automaticamente ou com sua permissão.

Além disso, é possível especificar o espaço (por padrão, 30 MB) no disco rígido para armazenar o histórico de atividades de programas, o que é necessário para reverter ações maliciosas.



4.13 Consultor de Arquivos e URLs

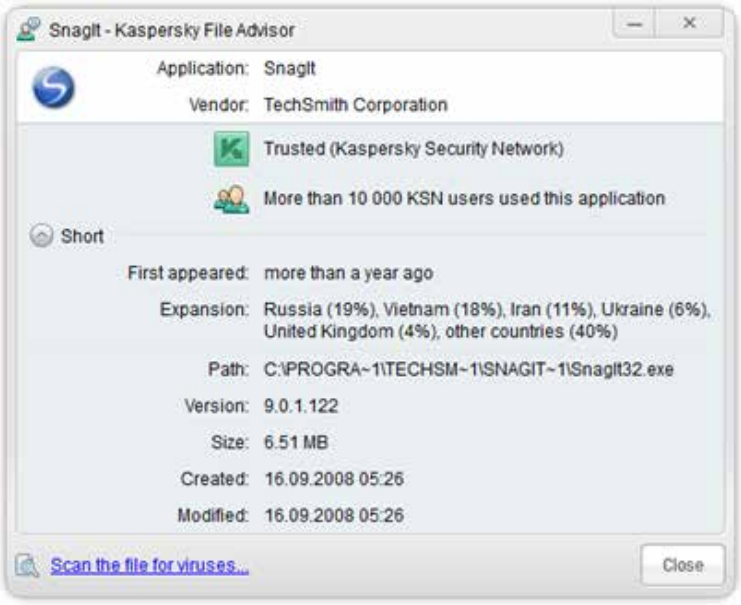
Agora, a reputação e o status de segurança de arquivos e sites estão ao alcance de suas mãos. Com um único clique do mouse, o **Consultor de Arquivos** usa as tecnologias baseadas em nuvem para verificar a segurança de qualquer arquivo que você queira acessar. E o **Consultor de URLs** adiciona marcas com códigos de cores a todos os links da Web para informar sobre o nível de perigo do link e das páginas seguintes. Pesquise na Web com a certeza de que não vai entrar em sites perigosos.

Consultor de Arquivos

Agora você pode verificar a reputação de qualquer arquivo com um único clique do mouse. Para fazer isso, clique com o botão direito do mouse no ícone do arquivo e selecione **Verificar reputação no KSN** (Kaspersky Security Network) no menu de contexto. Isso é prático, por exemplo, quando você baixou um arquivo da Internet, mas tem dúvidas sobre sua segurança e quer verificar sua reputação rapidamente.

Essa função fornece informações sobre nome do arquivo, tamanho, data de criação e da última modificação, classificação da ameaça, assinatura digital, geografia, distribuição e nível de confiança de outros usuários. Todos esses dados são exibidos no Windows Explorer ou na seção adicional da janela de verificação.

A principal vantagem desse recurso é que as informações da nuvem – as mais atualizadas disponíveis – são usadas para avaliar a reputação dos arquivos. Assim, é possível garantir que mesmo programas e arquivos novos são seguros.



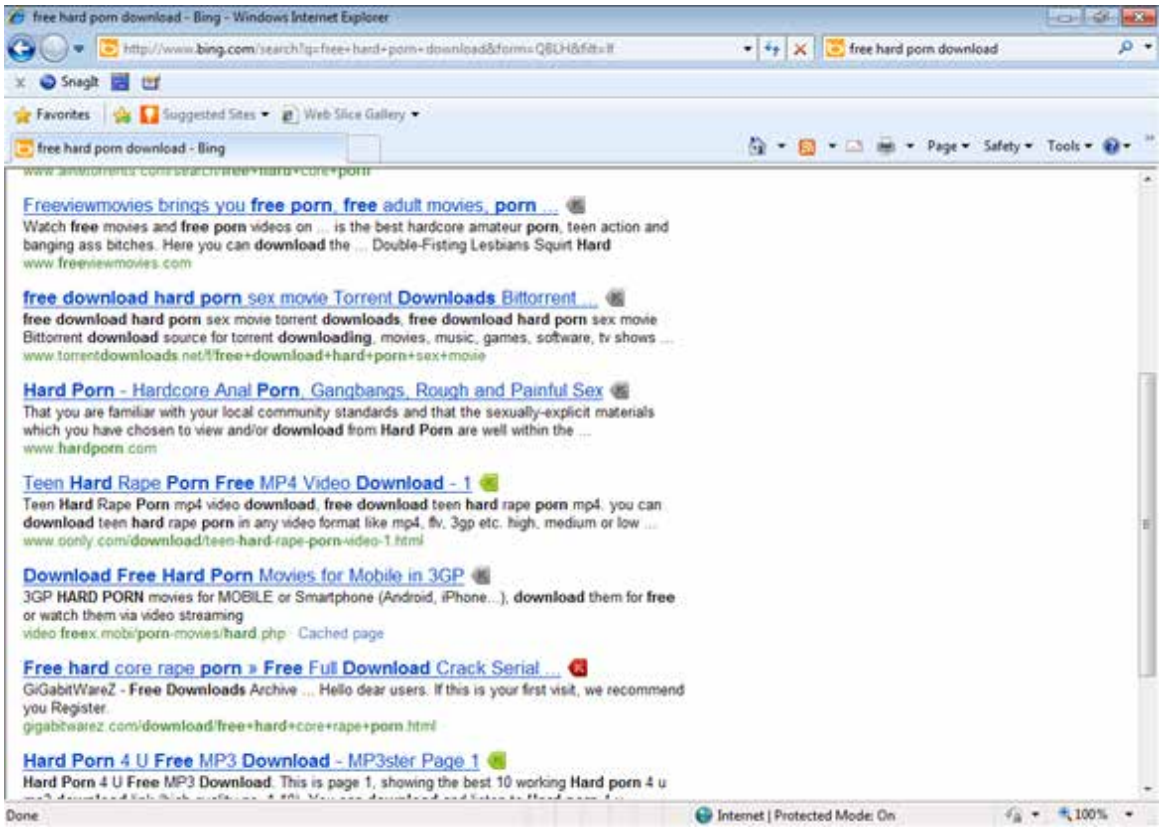
Consultor de URLs

O KIS 2013 inclui o módulo **Consultor de URLs,** que informa sobre links para sites suspeitos ou perigosos. O módulo consiste em uma barra de ferramentas para navegadores. Ele sinaliza os links para recursos infectado ou fraudulentos (phishing) usando um indicador colorido especial.

Os links podem ser verificados de duas maneiras:

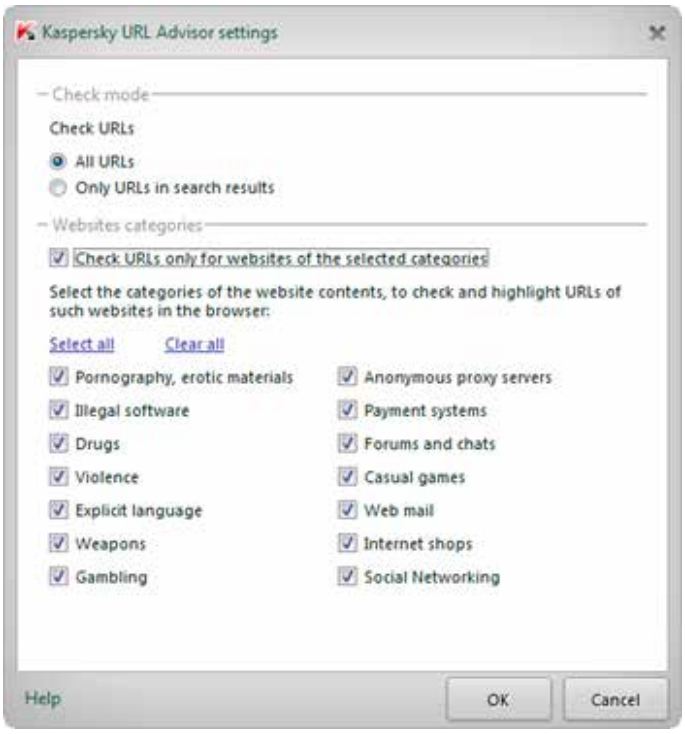
1. São verificados todos os links em todas as páginas da Web.
2. Modo leve: são verificados apenas os resultados de mecanismos de pesquisa e de pesquisas em sites.

O **Consultor de URLs** o informa sobre o perigo potencial que um site representa antes de você clicar no link.



O processo para determinar esse nível de perigo utiliza informações do banco de dados de URLs maliciosos e de phishing, e também dos bancos de dados localizados nos servidores da Kaspersky Lab (a chamada nuvem), produzindo pontuações de reputação para os URLs (o que é determinado, por exemplo, pelo fato das páginas da Web conterem código malicioso, quantos visitantes elas recebem ou se contêm links para sites suspeitos).

Além disso, o **Consultor de URLs** permite especificar categorias de sites indesejados (como “pornografia”, “crueldade e violência”, etc.).



A lista de navegadores compatíveis inclui:

- Internet Explorer 8, 9, 10
- Mozilla Firefox 9.x-12.x
- Google Chrome15.x-17.x
- Opera 12.61

4.14 Gadget

O KIS 2013 contém um gadget para o Windows Vista e o Windows 7. O gadget é um elemento da interface na área de trabalho do Windows que fornece acesso rápido às principais funções do produto. Agora não é mais necessário abrir a janela principal do aplicativo para executar as tarefas urgentes. Basta clicar no Gadget do Windows.

O gadget é exibido automaticamente na área de trabalho quando o Kaspersky Internet Security é instalado no Microsoft Windows 7. No Windows Vista, é necessário adicionar o gadget manualmente ao painel lateral (veja a documentação do sistema operacional).

5 Licenciamento e suporte

5.1 Informações de licenciamento

Informações sobre o período de validade de sua licença podem ser exibidas na parte central da janela principal do KIS 2013. Para obter mais informações, clique no link **Licenciamento** na parte inferior da janela.

O KIS 2013 inclui uma funcionalidade totalmente nova, a possibilidade de comprar uma licença diretamente no produto. Nesse caso, o KAV/KIS 2013 baixa informações sobre os produtos disponíveis e preços do servidor do parceiro, e você pode escolher o que precisa e comprar imediatamente usando a janela do programa. Não é necessário iniciar o navegador, nem visitar a loja online, o que economiza seu tempo. Para garantir que suas informações pessoais sejam protegidas adequadamente durante uma compra online, a segurança da conexão é verificada.

5.2 Suporte Técnico

Se você tiver dificuldades ou dúvidas técnicas sobre o produto, poderá entrar em contato com nosso Suporte Técnico 24x7 ou usar os recursos online com respostas a perguntas frequentes sobre a instalação e o uso do produto.