F-Secure Anti-Virus 2013

Conteúdo

Capítulo 1: Instalação.....5

Antes de instalar pela primeira vez.....6
Como instalar o produto pela primeira vez.....6
Como instalar e fazer o upgrade de aplicativos.....6
Ajuda e suporte.....7

Capítulo 2: Introdução.....9

Como utilizar as atualizações automáticas.....10
Verificar o status da atualização.....10
Alterar as configurações de conexão à internet.....10
Verificar o status da Rede de proteção em tempo real.....11
Como ver o que o produto fez.....11
Ver histórico de notificações.....11
Alterar as configurações de notificação.....11
Rede de proteção em tempo real.....12
O que é a Rede de proteção em tempo real.....12
Benefícios da Rede de proteção em tempo real.....12
Com quais dados você contribui.....13
Como protegemos sua privacidade.....14
Como ser um contribuidor da Rede de proteção em tempo real.....14
Perguntas sobre a Rede de proteção em tempo real.....15
Como sei que a minha assinatura é válida.....15
Centro de ações.....15
Ativar uma assinatura.....16

Capítulo 3: Introdução.....17

Exibir o status geral da minha proteção.....18
Ver as estatísticas do produto.....18
Lidar com atualizações do produto.....19
Ver versões do banco de dados.....19
Alterar as configurações de banda larga móvel.....19
O que são vírus e outros tipos de malware.....20
Vírus.....20
Spyware.....21
Rootkits.....21
Riskware.....21

Capítulo 4: Como proteger o computador contra malware.....23
Como verificar o meu computador.....24
Verificar arquivos automaticamente.....24
Verificar arquivos manualmente.....26
Verificar e-mails.....29
Ver os resultados da verificação.....30
Como excluir arquivos da verificação.....30
Excluir tipos de arquivo.....30
Excluir arquivos de acordo com o local.....31
Ver aplicativos excluídos.....32
Como utilizar a quarentena.....32
Ver itens em quarentena.....33
Restaurar itens da quarentena.....33
O que é o DeepGuard.....33
Ative ou desative o DeepGuard.....34
Permitir aplicativos que o DeepGuard bloqueou.....34
Usar o DeepGuard no modo de compatibilidade.....34
O que fazer com avisos de comportamento suspeito.....35

Capítulo

1

Instalação

Tópicos:

- *Antes de instalar pela primeira vez*
- *Como instalar o produto pela primeira vez*
- *Como instalar e fazer o upgrade de aplicativos*
- *Ajuda e suporte*

Antes de instalar pela primeira vez

Obrigado por escolher a F-Secure.

Para instalar o produto, é necessário o seguinte:

- O CD de instalação ou um pacote de instalação. Se estiver usando um netbook sem unidade de CD, é possível fazer o download do pacote de instalação de *www.f-secure.com/netbook*.
- Sua chave de assinatura.
- Uma conexão à internet.

Se tiver um produto de segurança de outro fornecedor, o instalador tentará removê-lo automaticamente. Se isso não acontecer, remova-o manualmente.

Nota: Se tiver mais de uma conta no computador, faça login com privilégios de administrador quando instalar.

Como instalar o produto pela primeira vez

Instruções para instalar o produto.

Siga estas instruções para instalar o produto:

1. Insira o CD ou clique duas vezes no instalador do qual fez download na internet.

   Se o CD não for iniciado automaticamente, vá ao Windows Explorer, clique duas vezes no ícone do CD-ROM e clique duas vezes no arquivo de instalação para iniciar a instalação.

2. Siga as instruções na tela.

   - Se tiver adquirido o produto em uma loja e ele vier em CD, você poderá encontrar a chave de assinatura na capa do Guia de instalação rápida.
   - Se você fez o download do produto da F-Secure eStore, a chave de assinatura vem inclusa no e-mail de confirmação da compra.

   Seu computador talvez precise ser reiniciado antes de validar sua assinatura e fazer o download das últimas atualizações da internet. Se estiver instalando a partir do CD, lembre-se de remover o CD de instalação antes de reiniciar seu computador.

Como instalar e fazer o upgrade de aplicativos

Instruções para ativar sua nova assinatura.

Siga estas instruções para ativar sua nova assinatura ou para instalar um novo aplicativo usando o launch pad:

Nota: Você pode encontrar o ícone do launch pad na bandeja de sistema do Windows.

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Ver minhas assinaturas**
3. Em **Minhas assinaturas**, vá para a página **Status da assinatura** e clique em **Ativar assinatura**.
   A janela **Ativar assinatura** é aberta.

4. Insira sua chave de assinatura para o aplicativo e clique em **OK**.
5. Após sua assinatura ser validada e ativada, clique em **Fechar**.
6. Em **Minhas assinaturas**, vá para a página **Status da assinatura**. Se a instalação não for iniciada automaticamente, siga estas instruções:
   a) Clique em **Instalar**.
      A janela de instalação é aberta.
   b) Clique em **Avançar**.
      O download do aplicativo é feito e a instalação é iniciada.
   c) Quando a instalação for concluída, clique em **Fechar**.

A nova assinatura foi ativada.

Ajuda e suporte

Você pode acessar a ajuda do produto on-line clicando no ícone Ajuda ou pressionando F1 em qualquer tela do produto.

Após registrar sua licença, você tem direito a serviços adicionais, como atualizações gratuitas e suporte do produto. Você pode registrar sua licença em *www.f-secure.com/register*.

Capítulo

2

Introdução

Tópicos:

- *Como utilizar as atualizações automáticas*
- *Como ver o que o produto fez*
- *Rede de proteção em tempo real*
- *Como sei que a minha assinatura é válida*

Informações sobre como começar a usar o produto.

Esta seção descreve como alterar as configurações comuns e gerenciar suas assinaturas por meio da barra inicial.

As configurações comuns da barra inicial são configurações que se aplicam a todos os programas instalados na barra inicial. Em vez de alterar as configurações separadamente em cada programa, você pode apenas editar as configurações comuns, que em seguida são usadas por todos os programas instalados.

As configurações comuns da barra inicial incluem:

- Downloads, onde é possível ver informações sobre quais atualizações foram instaladas e verificar manualmente se novas atualizações estão disponíveis.
- Configurações da conexão, onde é possível alterar como seu computador se conecta à internet.
- Notificações, onde é possível visualizar as notificações anteriores e definir qual tipo de notificação você deseja ver.
- Configurações privadas, onde é possível selecionar se o computador tem permissão para se conectar à Rede de proteção em tempo real.

Você também pode gerenciar suas assinaturas para programas instalados por meio da barra inicial.

Como utilizar as atualizações automáticas

A opção atualizações automáticas mantém a proteção no computador atualizada.

O produto salva as atualizações mais recentes no computador quando você está conectado à internet. Ele detecta o tráfego da rede e não interrompe o uso da internet mesmo que a conexão da rede seja lenta.

Verificar o status da atualização

Visualizar a data e a hora da última atualização.

Quando as atualizações automáticas estão ativadas, o produto recebe as últimas atualizações automaticamente quando você estiver conectado à internet.

Para verificar se as atualizações são as mais recentes:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Abrir configurações comuns**.
3. Selecione **Atualizações automáticas** > **Downloads**.
4. Clique em **Verificar agora**.
   O produto conecta-se à internet e procura as últimas atualizações. Se a proteção não estiver atualizada, ele recuperará as últimas atualizações.

   Nota: Se você estiver usando um modem ou tiver uma conexão ISDN com a internet, a conexão deverá estar ativa para verificar a presença de atualizações

Alterar as configurações de conexão à internet

Geralmente não há necessidade de alterar as configurações padrão, mas você pode configurar como o servidor fica conectado à internet para receber atualizações automaticamente.

Para alterar as configurações de conexão à internet:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Abrir configurações comuns**.
3. Selecione **Atualizações automáticas** > **Conexão**.
4. Na lista **Conexão à internet** selecione como o seu computador está conectado à internet.
   - Selecione **Supor que está sempre conectado** se houver uma conexão de rede permanente.

     Nota: Se, na realidade, o seu computador não tiver uma conexão de rede permanente e estiver configurado para discagem sob demanda, a seleção de **Supor que está sempre conectado** poderá resultar em várias discagens.
   - Selecione **Detectar conexão** para recuperar atualizações somente quando o produto detectar uma conexão de rede ativa.
   - Selecione **Detectar tráfego** para recuperar atualizações somente quando o produto detectar outro tráfego de rede.

     Dica: Se houver uma configuração de hardware incomum que faça a configuração **Detectar conexão** detectar uma conexão de rede ativa mesmo quando ela não existe, opte pela seleção de **Detectar tráfego**.

5. Na lista **Proxy HTTP**, selecione se deseja que o computador use um *servidor proxy* para se conectar à internet.
   - Selecione **Sem proxy HTTP** se o seu computador estiver conectado diretamente à internet.
   - Selecione **Configurar proxy HTTP manualmente** para definir as configurações do *Proxy HTTP*.
   - Selecione **Usar o proxy HTTP de meu navegador** para usar as mesmas configurações do *Proxy HTTP* que você definiu no seu navegador da web.

Verificar o status da Rede de proteção em tempo real

Para funcionar adequadamente, muitos recursos do produto dependem da conectividade com a rede de Proteção em tempo real.

Se houver problemas de rede ou se o firewall bloquear o tráfego da Rede de proteção em tempo real, o status será "desconectada". Se nenhum dos recursos instalado necessitarem do acesso à Rede de proteção em tempo real, o status é "sem uso".

Para verificar o status:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Abrir configurações comuns**.
3. Selecione **Atualizações automáticas** > **Conexão**.

Em **Rede de proteção em tempo real**, você pode ver o status atual da Rede de proteção em tempo real.

Como ver o que o produto fez

Veja quais ações o produto realizou para proteger seu computador na página **Notificações**.

O produto exibirá uma notificação quando realizar uma ação. Por exemplo, quando encontrar um vírus e bloqueá-lo. Algumas notificações também podem ser enviadas por seu fornecedor de serviços, por exemplo para informar sobre novos serviços que estão disponíveis.

Ver histórico de notificações

Você pode ver quais notificações foram exibidas no histórico de notificações

Para ver o histórico de notificações:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Abrir configurações comuns**.
3. Selecione **Outro** > **Notificações**.
4. Clique em **Mostrar histórico de notificações**.
   A lista do histórico de notificações é aberta.

Alterar as configurações de notificação

É possível selecionar quais tipos de notificação você deseja que o produto exiba.

Para alterar as configurações de notificação:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.

2. Selecione **Abrir configurações comuns**.
3. Selecione **Outro** > **Notificações**.
4. Marque ou desmarque **Permitir mensagens do programa** para ativar ou desativar as mensagens do programa.

   Quando esta configuração estiver ativada, o produto mostrará notificações dos programas instalados.
5. Marque ou desmarque **Permitir mensagens promocionais** para ativar ou desativar mensagens promocionais.
6. Clique em **OK**.

Rede de proteção em tempo real

Este documento descreve a Rede de proteção em tempo real, um serviço on-line da F-Secure Corporation que identifica aplicativos e sites livres de infecção enquanto fornece proteção contra vulnerabilidades de sites e malware.

O que é a Rede de proteção em tempo real

A Rede de proteção em tempo real é um serviço on-line que fornece respostas rápidas às ameaças vindas da internet.

Como um contribuidor da Rede de proteção em tempo real, você pode nos ajudar a fortalecer a proteção contra ameaças novas e que vão surgindo com o tempo. A Rede de proteção em tempo real coleta estatísticas de determinados aplicativos suspeitos, maliciosos ou desconhecidos e o que fazem no seu aparelho. Essas informações são anônimas e enviadas à F-Secure Corporation para análise combinada de dados. Usamos as informações analisadas para melhorar a segurança em seu aparelho contra as últimas ameaças e arquivos maliciosos.

Como funciona a Rede de proteção em tempo real

Como um contribuidor da Rede de proteção em tempo real, você pode fornecer informações sobre aplicativos e sites desconhecidos e aplicativos maliciosos em sites. A Rede de proteção em tempo real não rastreia a sua atividade na rede ou coleta informações sobre sites que já foram analisados e não coleta informações sobre aplicativos limpos que estiverem instalados no seu computador.

Se você não quiser contribuir com esses dados, a Rede de proteção em tempo real não coleta informações de aplicativos instalados ou sites visitados. Entretanto, o produto precisa consultar os servidores da F-Secure para conhecer a reputação de aplicativos, sites, mensagens e outros objetos. A consulta é feita usando uma soma de verificação criptografada na qual o objeto consultado em si não é enviado para a F-Secure. Não rastreamos dados por usuário. Apenas o contador de visitas do arquivo ou site aumenta.

Não é possível interromper completamente todo o tráfego de rede para a Rede de proteção em tempo real, já que é parte integral da proteção fornecida pelo produto.

Benefícios da Rede de proteção em tempo real

Com a Rede de proteção em tempo real, você terá proteção mais rápida e precisa contra as últimas ameaças e não receberá alertas desnecessários para aplicativos suspeitos que não são maliciosos.

Como contribuidor da Rede de proteção em tempo real, você pode nos ajudar a encontrar malwares novos e não detectados e remover possíveis falsos positivos do nosso banco de dados de definição de vírus.

Todos os participantes da Rede de proteção em tempo real ajudam uns aos outros. Quando a Rede de proteção em tempo real encontra um aplicativo suspeito em seu aparelho, você se beneficia dos resultados da análise feita quando o mesmo aplicativo foi encontrado em outros aparelhos. A Rede de proteção em tempo real melhora o desempenho geral do seu aparelho, já que o produto de segurança instalado não

precisa verificar novamente os aplicativos que a Rede de proteção em tempo real já analisou e descobriu que não estão infectados. De maneira parecida, informações sobre sites maliciosos e mensagens em massa que não foram solicitadas são compartilhadas por meio da Rede de proteção em tempo real, e podemos fornecer a você proteção mais precisa contra vulnerabilidades de sites e mensagens com spam.

Quanto mais pessoas contribuírem com a Rede de proteção em tempo real, melhor protegidos estarão os participantes individuais.

Com quais dados você contribui

Como um contribuidor da Rede de proteção em tempo real, você fornece informações sobre aplicativos armazenados em seu aparelho e os sites que você visita, para que a Rede de proteção em tempo real possa fornecer proteção contra os sites suspeitos e aplicativos maliciosos mais recentes.

Análise da reputação do arquivo

A Rede de proteção em tempo real coleta informações apenas sobre aplicativos que não têm reputação conhecida e sobre arquivos que são suspeitos ou são identificados como malware.

A Rede de proteção em tempo real coleta informações anônimas de aplicativos limpos e suspeitos do seu dispositivo. A Rede de proteção em tempo real coleta apenas informações de arquivos executáveis (como arquivos executáveis portáteis na plataforma Windows, que têm extensões de arquivo .cpl, .exe, .dll, .ocx, .sys, .scr e .drv).

As informações coletadas incluem:

- o caminho do arquivo de onde o aplicativo está em seu aparelho,
- o tamanho do arquivo e quando ele foi criado ou modificado,
- atributos e privilégios de arquivo,
- informações da assinatura do arquivo,
- a versão atual do arquivo e a empresa que o criou,
- a origem do arquivo ou o URL do download e
- Resultados de análises de antivírus e do F-Secure DeepGuard de arquivos verificados e
- outras informações similares.

A Rede de proteção em tempo real nunca coleta informações dos seus documentos pessoais, a menos que eles estejam infectados. Para qualquer tipo de arquivo malicioso, ele coleta o nome do status de infecção e desinfecção do arquivo.

Com a Rede de proteção em tempo real você também pode enviar aplicativos suspeitos para serem analisados. Apenas aplicativos em arquivos portáteis executáveis podem ser enviados. A Rede de proteção em tempo real nunca coleta informações de seus documentos pessoais e eles nunca são automaticamente enviados para análise.

Envio de arquivos para análise

Com a Rede de proteção em tempo real, você também pode enviar aplicativos suspeitos para análise.

Você pode enviar aplicativos suspeitos individuais manualmente quando o produto solicitar que você faça isso. Você pode apenas enviar arquivos executáveis portáteis. A Rede de proteção em tempo real nunca faz upload de seus documentos pessoais.

Análise da reputação de sites

A Rede de proteção em tempo real não rastreia sua atividade na web ou coleta informações sobre sites que já foram analisados. Ela se certifica de que os sites visitados são seguros conforme você navega na web. Quando você visita um site, a Rede de proteção em tempo real verifica sua segurança e notifica você se o site estiver classificado como suspeito ou perigoso.

Se o site que você visitar contiver conteúdo malicioso ou uma vulnerabilidade conhecida, a Rede de proteção em tempo real coleta todo o URL do site para que o conteúdo da página da web possa ser analisado.

Se você visitar um site que ainda não foi classificado, a Rede de proteção em tempo real coleta nomes de domínio e subdomínio e, em alguns casos, o caminho para a página visitada, para que o site possa ser analisado e classificado. Todos os parâmetros de URL que possam de alguma maneira ser vinculados pessoalmente a você são removidos para proteger sua privacidade.

Nota: A Rede de proteção em tempo real não classifica ou analisa páginas da web em redes privadas, portanto nunca coleta quaisquer informações em endereços de rede IP privados (por exemplo, intranets corporativas).

Análise de informações do sistema

A Rede de proteção em tempo real coleta o nome e a versão do seu sistema operacional, informações sobre a conexão à internet e as estatísticas de uso da Rede de proteção em tempo real (por exemplo, o número de vezes que reputações de sites foram consultadas e a média de tempo para a consulta retornar um resultado) para que possamos monitorar e melhorar o serviço.

Como protegemos sua privacidade

Transferimos as informações de forma segura e removemos automaticamente quaisquer informações pessoais que os dados possam conter.

A Rede de proteção em tempo real remove os dados que possam identificá-lo antes de enviá-los à F-Secure e todas as informações coletadas são criptografadas durante a transferência para proteger os dados de acesso sem autorização. As informações coletadas não são processadas individualmente: são agrupadas com informações de outros contribuidores da Rede de proteção em tempo real. Todos os dados são analisados estatisticamente e de forma anônima, o que significa que não há maneira de os dados serem associados a você.

Quaisquer informações que possam identificar você não são incluídas nos dados coletados. A Rede de proteção em tempo real não coleta endereços IP privados ou suas informações particulares, como endereços de e-mail, nomes de usuário ou senhas. Embora nos esforcemos para remover todos os dados pessoalmente identificáveis, é possível que parte desses dados continue nas informações coletadas. Nesses casos, não procuraremos usar os dados coletados sem intenção para identificar você.

Aplicamos medidas de segurança restritas e medidas técnicas, administrativas e físicas para proteger as informações coletadas quando são transferidas, armazenadas e processadas. As informações são armazenadas em locais seguros e em servidores controlados por nós, localizados em nossos escritórios ou nos escritórios de nossos subcontratados. Apenas pessoal autorizado pode acessar as informações coletadas.

A F-Secure pode compartilhar os dados coletados com suas afiliadas, subcontratadas, distribuidores e parceiros, mas sempre em formato anônimo e não-identificável.

Como ser um contribuidor da Rede de proteção em tempo real

Você nos ajuda a melhorar a Rede de proteção em tempo real contribuindo com informações sobre programas e sites maliciosos.

Você pode escolher participar da Rede de proteção em tempo real durante a instalação. Com as configurações padrão de instalação, você contribui com dados para a Rede de proteção em tempo real. É possível alterar essa configuração mais tarde no produto.

Siga estas instruções para alterar as configurações da Rede de proteção em tempo real:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Abrir configurações comuns**.
3. Selecione **Outro** > **Privacidade**.

4. Marque a caixa de seleção de participação para se tornar um contribuidor da Rede de proteção em tempo real.

Perguntas sobre a Rede de proteção em tempo real

Informações de contato para solucionar dúvidas sobre a Rede de proteção em tempo real.

Se você tiver mais dúvidas sobre a Rede de proteção em tempo real, entre em contato com:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlândia

http://www.f-secure.com/en/web/home_global/support/contact

A versão mais recente da nossa política está sempre disponível em nosso site.

Como sei que a minha assinatura é válida

O tipo e status da assinatura são mostrados na página **Status da assinatura**.

Quando a assinatura estiver prestes a expirar ou se já tiver expirado, o status da proteção geral do programa no ícone correspondente da barra inicial é alterado.

Para verificar a validade da assinatura:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Ver minhas assinaturas**.
3. Selecione **Status da assinatura** para ver informações sobre suas assinaturas e programas instalados.
4. Selecione **Status da instalação** para ver quais programas estão disponíveis para serem instalados.

O status da assinatura e a data de expiração também são mostrados na página **Estatísticas**.Se a assinatura já expirou, é necessário renová-la para continuar a receber atualizações e a utilizar o produto.

Nota: Quando a assinatura já tiver expirado, o ícone de status do produto fica piscando na bandeja do sistema.

Centro de ações

O centro de ações mostra as notificações importantes que exigem sua atenção.

Se sua assinatura expirou ou está prestes a expirar, o centro de ações notifica você sobre isso. A cor do plano de fundo e a mensagem do centro de ações depende do seu tipo e status de assinatura:

- Se sua assinatura estiver prestes a expirar, e houver assinaturas gratuitas disponíveis, a mensagem tem um plano de fundo branco e um botão **Ativar**.
- Se sua assinatura estiver prestes a expirar e não houver assinaturas gratuitas disponíveis, a mensagem tem um plano e fundo amarelo e botões**Comprar** e **Inserir chave**. Se já tiver comprado uma nova assinatura, clique em **Inserir chave** para fornecer a chave de assinatura e ativar sua nova assinatura.

- Se sua assinatura tiver expirado, e houver assinaturas gratuitas disponíveis, a mensagem tem um plano de fundo vermelho e um botão **Ativar**.
- Se sua assinatura tiver expirado e não houver assinaturas gratuitas disponíveis, a mensagem tem um plano de fundo vermelho e botões **Comprar** e **Inserir chave**. Se você já tiver comprado uma nova assinatura, clique em **Inserir chave** para fornecer a chave de assinatura e ativar sua nova assinatura.

Nota: O link **Mostrar histórico de notificações** no centro de ações mostra uma lista de mensagens de notificação do produto, e não mensagens anteriores do centro de ações.

Ativar uma assinatura

Quando você tem uma nova chave de assinatura ou código de campanha para um produto, é necessário ativá-lo.

Para ativar uma assinatura:

1. No launch pad, clique com o lado direito do mouse no ícone à direita.
   Um menu pop-up é aberto.
2. Selecione **Ver minhas assinaturas**.
3. Escolha uma das seguintes opções:
   - Clique em **Ativar assinatura**.
   - Clique em **Ativar código da campanha**.
4. Na caixa de diálogo que é aberta, insira a nova chave de assinatura ou código de campanha e clique em **OK**.

   Dica: Se você recebeu a chave de assinatura por e-mail, copie-a da mensagem de e-mail e cole-a no campo.

Após inserir a nova chave de assinatura, a data de validade da nova assinatura é exibida na página **Status da assinatura**.

Capítulo

3

Introdução

Tópicos:

- *Exibir o status geral da minha proteção*
- *Ver as estatísticas do produto*
- *Lidar com atualizações do produto*
- *O que são vírus e outros tipos de malware*

Este produto protege seu computador de vírus e outros aplicativos perigosos.

O produto verifica arquivos, analisa aplicativos e é atualizado automaticamente. Ele não requer nenhuma ação sua.

Exibir o status geral da minha proteção

A página **Status** mostra uma visão geral rápida dos recursos do produto instalados e os respectivos status no momento.

Para abrir a página **Status**:

Na página principal, clique em **Status**.

A página **Status** é aberta.

Os ícones mostram o status do programa e seus recursos de segurança.

Ícone de status	Nome do status	Descrição
	OK	O computador está protegido. O recurso está ativado e funcionando adequadamente.
	Informações	O produto informa a respeito de um status especial de um recurso. Por exemplo, o recurso está sendo atualizado.
	Aviso	O computador não está totalmente protegido. Por exemplo, o produto não recebeu atualizações por um longo tempo, ou o status de um recurso requer atenção.
	Erro	O computador não está protegido Por exemplo, sua assinatura expirou ou um recurso crítico está desativado.
	Desativado	Um recurso não crítico está desativado.

Ver as estatísticas do produto

É possível ver o que o produto fez desde a sua instalação na página **Estatísticas**.

Para abrir a página **Estatísticas**:

Na página principal, clique em **Estatísticas**.

A página **Estatísticas** é aberta.

- A opção **Última verificação de atualização realizada com êxito** mostra o horário da última atualização.

- A opção **Verificação de vírus e spyware** mostra quantos arquivos o produto verificou e limpou desde a instalação.
- **Aplicativos** mostra quantos programas o DeepGuard permitiu ou bloqueou desde a instalação.
- **Conexões do firewall** exibe o número de conexões permitidas e bloqueadas desde a instalação.
- A **filtragem de spam e phishing** mostra quantas mensagens de e-mail o produto detectou como e-mails válidos e quantas como mensagens de spam.

Lidar com atualizações do produto

O produto mantém a proteção atualizada automaticamente.

Ver versões do banco de dados

Você pode ver os números das versões e os momentos das últimas atualizações na página **Atualizações do banco de dados**.

Para abrir a página **Atualizações do banco de dados**:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Outras configurações** > **Versões do banco de dados**.

A página **Versões do banco de dados** exibe a data mais recente em que as definições de vírus e spyware, o DeepGuard e a filtragem de spam e phishing foram atualizadas e o número das versões.

Alterar as configurações de banda larga móvel

Selecione se você deseja fazer o download de atualizações de segurança quando usar banda larga móvel.

Nota: Este recurso está disponível apenas para o Microsoft Windows 7.

Por padrão, o download das atualizações de segurança é sempre feito quando você está usando a rede da sua operadora. Entretanto, as atualizações são suspensas quando você visita a rede de outra operadora. Isso acontece porque os preços das conexões podem variar entre as operadoras, por exemplo, em países diferentes. É recomendável manter esta configuração dessa maneira se desejar economizar largura de banda e, possivelmente, também os gastos durante a sua visita.

Nota: Esta configuração se aplica apenas a conexões de banda larga móvel. Quando o computador está conectado a uma rede fixa ou sem fio, o produto é automaticamente atualizado.

Para alterar a configuração:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Outras configurações** > **Banda larga móvel** > **Fazer download de atualizações de seguranças**.
3. Selecione a opção de atualização preferida para conexões móveis:
   - **Apenas na rede doméstica da operadora**

     O download das atualizações de segurança é sempre feito quando você está usando a rede da sua operadora. Quando você visita a rede de outra operadora, as atualizações são suspensas.

Recomendamos que você selecione esta opção para manter seu produto de segurança atualizado gastando apenas o esperado.

- **Nunca**

  Não é feito o download de nenhuma atualização quando uma banda larga móvel estiver sendo usada.

- **Sempre**

  O download das atualizações é sempre feito, sem importar a rede usada no momento. Selecione essa opção se você desejar se certificar que a segurança do seu computador está sempre atualizada independentemente dos custos.

4. Se você quiser decidir separadamente toda vez que sair da rede da sua operadora, selecione **Perguntar toda vez que eu sair da rede doméstica da minha operadora**.

Atualizações de segurança suspensas

As atualizações de segurança podem ser suspensas quando você usa banda larga móvel fora da cobertura da rede da sua operadora.

Neste caso, você pode ver a notificação **Suspenso** no canto inferior direito da sua tela. As atualizações são suspensas porque os preços das conexões podem variar entre as operadoras, por exemplo, em países diferentes. É recomendável manter esta configuração dessa maneira se desejar economizar largura de banda e, possivelmente, também os gastos durante a sua visita. Entretanto, se ainda desejar alterar as configurações, clique no link **Alterar**.

Nota:

Este recurso está disponível apenas para o Microsoft Windows 7.

O que são vírus e outros tipos de malware

O malware é um programa especialmente criado para danificar o seu computador, usar o computador para objetivos ilícitos sem o seu conhecimento ou roubar informações do computador.

O malware pode:

- controlar o seu navegador da web,
- redirecionar suas tentativas de busca,
- mostrar anúncios indesejados,
- rastrear os sites que você acessa,
- roubar informações pessoais, como suas informações bancárias,
- usar seu computador para enviar spam e
- usar seu computador para atacar outros computadores.

O malware também pode fazer com que o computador fique lento e instável. Você talvez suspeite que exista algum *malware* em seu computador se ele repentinamente tornar-se lento e travar com frequência.

Vírus

Geralmente, os vírus são programas que podem se anexar a arquivos e se multiplicar repetidamente; eles podem alterar e substituir os conteúdos de outros arquivos de modo a danificar o computador.

Um *vírus* é um programa que geralmente é instalado sem o seu conhecimento no computador. Após instalado, o vírus tenta multiplicar-se. O vírus:

- usa alguns recursos do sistema do computador,
- pode alterar ou danificar arquivos no computador,

- provavelmente tenta usar seu computador para infectar outros computadores,
- talvez permita que seu computador seja usado para objetivos ilícitos.

Spyware

Spywares são programas que coletam suas informações pessoais.

Os spywares podem coletar informações pessoais, inclusive:

- sites da internet que você acessou,
- endereços de e-mail em seu computador,
- senhas ou
- números de cartões de crédito.

Os spywares quase sempre se instalam sem a sua permissão explícita. O spyware pode ser instalado junto com um programa útil ou enganando-o para clicar em uma opção em uma janela pop-up falsa.

Rootkits

Os rootkits são programas que dificultam a localização de outro *malware*.

Os rootkits ocultam arquivos e processos. Em geral, eles fazem isso para ocultar atividades maliciosas no computador. Quando um rootkit oculta um *malware* fica difícil descobrir se o computador tem um malware.

Este produto possui um scanner de rootkit que verifica especificamente a presença de rootkits, o que dificulta a ocultação do *malware*.

Riskware

O riskware não é desenvolvido especificamente para danificar o computador, mas ele pode danificá-lo se for mal utilizado.

O riskware não é exatamente um malware. Programas riskware executam algumas funções úteis, no entanto, potencialmente perigosas.

Exemplos de programas riskware:

- programas para mensagens instantâneas, como o IRC (Internet Relay Chat),
- programas para transferência de arquivos pela internet de um computador para outro,
- ou programas de telefone pela Internet como o VoIP (*Protocolo Voice over Internet*) .
- Softwares de acesso remoto, como o VNC.
- scareware, aqueles programas que podem tentar assustar ou enganar os usuários para que comprem software de segurança falso ou
- softwares projetados para burlar verificações de CD e proteções de cópias.

Se você explicitamente instalou o programa e o configurou corretamente, é menos provável que ele seja perigoso.

Se o riskware foi instalado sem o seu conhecimento, é bem provável que tenha sido instalado com intenções maliciosas e deverá ser removido.

Capítulo

4

Como proteger o computador contra malware

Tópicos:

- *Como verificar o meu computador*
- *Como excluir arquivos da verificação*
- *Como utilizar a quarentena*
- *O que é o DeepGuard*

A verificação de vírus e spyware protege o computador contra programas que podem roubar informações pessoais, danificar o computador ou utilizá-lo para finalidades ilegais.

Por padrão, todos os tipos de malware são imediatamente eliminados quando encontrados, para que não possam causar danos.

Por padrão, a verificação de vírus e spyware verifica automaticamente os discos rígidos locais, qualquer mídia removível (como unidades portáteis ou CDs) e conteúdo cujo download foi feito para o computador. Você pode configurá-la para também verificar automaticamente os seus e-mails.

A verificação de vírus e spyware também observa o computador quanto a quaisquer alterações que possam indicar *malware*. Se quaisquer alterações perigosas do sistema, por exemplo, configurações do sistema ou tentativas de alterar processos importantes do sistema, forem encontradas, o DeepGuard interromperá a execução desse programa, pois é provável que seja um *malware*.

Como verificar o meu computador

Quando a Verificação de vírus e spyware está ativada, ela verifica seu computador automaticamente em busca de arquivos perigosos. Você também pode verificar arquivos manualmente e configurar verificações agendadas.

Recomendamos manter a Verificação de vírus e spyware ativada permanentemente. Verifique seus arquivos manualmente quando desejar certificar-se de que não há arquivos perigosos em seu computador ou se desejar verificar arquivos que tiver excluído da verificação em tempo real.

Ao configurar uma verificação agendada, a Verificação de vírus e spyware remove arquivos perigosos de seu computador em momentos especificados.

Verificar arquivos automaticamente

A verificação em tempo real protege o computador ao verificar todos os arquivos quando são acessados e ao bloquear o acesso aos arquivos que contêm *malware*.

Quando seu computador tenta acessar um arquivo, a Verificação em tempo real verifica o arquivo em busca de malware antes de permitir que seu computador acesse o arquivo. Se a Verificação em tempo real encontrar conteúdo perigoso, colocará o arquivo na quarentena antes que possa causar quaisquer danos.

A Verificação em tempo real afeta o desempenho do meu computador?

Normalmente, o processo de verificação é imperceptível, pois é rápido e não utiliza muitos recursos do sistema. A quantidade de tempo e de recursos do sistema que a verificação em tempo real utiliza depende, por exemplo, do conteúdo, do local e do tipo de arquivo.

Arquivos cuja verificação é demorada:

- Arquivos em unidades removíveis como CDs, DVDs e unidades USB portáteis.
- Os arquivos compactados, como os arquivos *.zip*.

  Nota: Arquivos compactados não são verificados por padrão.

A verificação em tempo real pode tornar o computador mais lento se:

- você tiver um computador que não atende aos requisitos de sistema ou se
- você acessar muitos arquivos ao mesmo tempo. Por exemplo, quando abrir um diretório que contém muitos arquivos que precisam ser verificados.

Ativar a verificação em tempo real

Mantenha a verificação em tempo real ativada para impedir que *malwares* danifiquem o computador.

Para ativar ou desativar a verificação em tempo real:

1. Na página principal, clique em **Status**.
2. Clique em **Alterar configurações nesta página**.

   Nota: Você precisa de direitos de administrador para desativar os recursos de segurança.

3. Ative ou desative **Verificação de vírus e spyware**.
4. Clique em **Fechar**.

Lidar com arquivos perigosos automaticamente

A verificação em tempo real pode lidar com arquivos perigosos automaticamente sem fazer nenhuma pergunta.

Para permitir que a verificação em tempo real lide com arquivos perigosos automaticamente:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Selecione **Resolver o que fazer com arquivos perigosos automaticamente**.

Se escolher não resolver o que fazer com arquivos perigosos automaticamente, a verificação em tempo real perguntará o que você deseja fazer com um arquivo perigoso quando ele for encontrado.

Lidar com spyware

A Verificação de vírus e spyware bloqueia spyware imediatamente, quando o aplicativo tenta ser iniciado.

Antes que um aplicativo spyware possa iniciar, o produto o bloqueia e permite que você decida o que fazer com ele.

Escolha uma das seguintes ações quando um spyware for encontrado:

Ação a ser realizada	O que acontece com o spyware
Resolver automaticamente	Quando o produto decide a melhor ação a ser tomada com base no spyware que foi encontrado.
Colocar o spyware na quarentena	Move o spyware para a quarentena, onde não poderá danificar seu computador.
Excluir o spyware	Remove todos os arquivos relacionados ao spyware do computador.
Apenas bloquear o spyware	Bloqueia o acesso ao spyware mas deixa-o no computador.
Excluir o spyware da verificação	Permite que o spyware seja executado e o exclui da verificação no futuro.

Lidar com riskware

A Verificação de vírus e spyware bloqueia riskware imediatamente, quando o aplicativo tenta ser iniciado.

Antes que um aplicativo riskware possa iniciar, o produto o bloqueia e permite que você decida o que fazer com ele.

Escolha uma das seguintes ações quando um riskware for encontrado:

Ação a ser realizada	O que acontece com o riskware
Apenas bloquear o riskware	Bloqueia o acesso ao riskware mas deixa-o no computador.
Colocar o riskware na quarentena	Move o riskware para a quarentena, onde não poderá danificar seu computador.
Excluir o riskware	Remove todos os arquivos relacionados ao riskware do computador.
Excluir o riskware da verificação	Permite que o riskware seja executado e o exclui da verificação no futuro.

Remover cookies de rastreamento automaticamente

Ao remover cookies de rastreamento, você evita que sites possam rastrear os sites que você acessa na internet.

Os cookies de rastreamento são pequenos arquivos que permitem que sites da web registrem os sites que você visita. Siga estas instruções para evita que cookies de rastreamento sejam instalados em seu computador.

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Selecione **Remover cookies de rastreamento**.
4. Clique em **OK**.

Verificar arquivos manualmente

Você pode verificar seus arquivos manualmente, por exemplo, quando conectar um dispositivo externo ao seu computador, para garantir que não contenha malware.

Como iniciar a verificação manual

É possível verificar todo o computador, um tipo específico de *malware* ou um local específico.

Se você suspeitar que há um determinado tipo de *malware*, poderá verificar somente esse tipo. Se você suspeitar de um determinado local em seu computador, poderá verificar somente aquela seção. Essas verificações serão concluídas de forma mais rápida do que uma verificação de todo o computador.

Para iniciar a verificação manual em seu computador:

1. Na página principal, clique na seta logo abaixo de **Verificar**.

   As opções de verificação são mostradas.

2. Selecione o tipo de verificação.

   Selecione **Alterar configurações da verificação** para otimizar como a verificação manual verifica o computador em busca de vírus e outros aplicativos perigosos.

3. Se você selecionou **Escolher o que verificar**, uma janela será aberta na qual é possível selecionar qual local verificar.
   O **Assistente de verificação** será aberto.

Tipos de verificação

É possível verificar todo o computador, um tipo específico de malware ou um local específico.

A lista a seguir mostra os diferentes tipos de verificação:

Tipo de verificação	O que é verificado	Quando utilizar este tipo
Verificação de vírus e spyware	Partes do computador em busca de vírus, spyware e riskware	Este tipo de verificação é muito mais rápida que uma verificação completa. Ela pesquisa apenas as partes do sistema que contenham arquivos de programas instalados. Esse tipo de verificação é recomendado se você desejar verificar rapidamente se o computador está limpo, porque ele pode encontrar e remover com eficiência qualquer malware ativo no computador.
Verificação completa do computador	Todo o computador (discos rígidos internos e externos) em busca de vírus, spyware e riskware	Para ter certeza absoluta de que não há malware ou riskware em seu computador. Este tipo de verificação demora mais tempo para ser concluída. Ela combina a verificação rápida de malware e a verificação de disco rígido. Ela também verifica os itens que possivelmente estão ocultos por rootkit.

Tipo de verificação	O que é verificado	Quando utilizar este tipo
Escolher o que verificar	Um arquivo ou pasta específica em busca de vírus, spyware e riskware	Se você suspeitar que há malware em um local específico de seu computador, por exemplo, o local contém downloads de fontes potencialmente perigosas, como redes ponto a ponto de compartilhamento de arquivos. A duração da verificação dependerá do tamanho do destino que você verificar. A verificação termina mais rapidamente se, por exemplo, uma pasta que contém somente poucos arquivos pequenos for verificada.
Verificação de rootkit	Locais importantes do sistema onde um item suspeito pode significar um problema de segurança. Verifica se há arquivos, pastas, unidades ou processos ocultos	Quando você suspeitar que um rootkit pode estar instalado no computador. Por exemplo, se um malware foi recém-detectado no computador e você deseja certificar-se de que ele não instalou um rootkit.

Verificar no Windows Explorer

É possível verificar discos, pastas e arquivos em busca de *vírus*, *spyware* e *riskware* no Windows Explorer.

Para verificar um disco, pasta ou arquivo:

1. Coloque o ponteiro do mouse e clique com o botão direito no disco, pasta ou arquivos que você deseja verificar.
2. No menu que é exibido quando você clica com o botão direito do mouse, selecione **Verificar se há vírus nas pastas**. (O nome da opção depende do que está sendo verificado: um disco, uma pasta ou um arquivo).
   A janela **Assistente de verificação** é aberta e a verificação é iniciada.

Se um *vírus* ou um *spyware* for encontrado, o **Assistente de verificação** levará você pelas etapas de remoção.

Selecione os arquivos para verificar

Você pode selecionar os tipos de arquivo que você deseja verificar em busca de *vírus* e *spywares* em verificações manuais ou agendadas.

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Outras configurações** > **Verificação manual**.
3. Em **Opções de verificação**, selecione a partir das seguintes configurações:

Verificar apenas os tipos de arquivo conhecidos	Para verificar apenas aqueles tipos de arquivos com maior probabilidade de conter infecções, como arquivos executáveis, por exemplo. Selecionar esta opção também torna a verificação mais rápida. Os arquivos com as seguintes extensões são verificados: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` e `.hqx`.

Verificar dentro de arquivos compactados	Para verificar pastas e arquivos compactados.
Usar heurística avançada	Para usar todas as heurísticas disponíveis durante a verificação para encontrar melhor malware novos ou desconhecidos. **Nota:** Se selecionar essa opção, a verificação levará mais tempo e podem ocorrer mais falsos positivos (arquivos inofensivos reportados como suspeitos).

4. Clique em **OK**.

Nota: Os arquivos excluídos na lista de itens excluídos não são verificados mesmo se você selecioná-los para serem verificados aqui.

O que fazer quando arquivos perigosos são encontrados

Selecione como deseja que os arquivos perigosos sejam tratados quando forem encontrados.

Para selecionar a ação a ser tomada quando conteúdo perigoso for encontrado durante a verificação manual:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Outras configurações** > **Verificação manual**.
3. Em **Quando vírus ou spyware for encontrado**, escolha uma das seguintes opções:

Opção	Descrição
Perguntar (padrão)	Você pode selecionar a ação a ser tomada para cada item encontrado durante a verificação manual.
Limpar os arquivos	O produto tenta desinfetar automaticamente os arquivos infectados encontrados durante a verificação manual. **Nota:** Se o produto não puder limpar o arquivo infectado, ele será colocado na quarentena (exceto quando encontrado na rede ou em unidades removíveis), para que não possa danificar o computador.
Colocar os arquivos em quarentena	O produto automaticamente coloca os arquivos perigosos encontrados durante a verificação manual na quarentena, onde não poderão danificar o computador.
Excluir os arquivos	O programa exclui qualquer arquivo perigoso encontrado durante a verificação manual.
Somente relatório	O programa deixa os arquivos perigosos encontrados durante a verificação manual como estão e registra a detecção no relatório de verificação. **Nota:** Se a verificação em tempo real estiver desativada, os malwares ainda poderão danificar o computador se você selecionar essa opção.

Nota: Quando arquivos perigosos são encontrados durante a verificação agendada, são limpos automaticamente.

Agendar uma verificação

Configure seu computador para verificar e remover vírus e outros aplicativos perigosos automaticamente quando você não estiver usando-o, ou configure a verificação para ser executada periodicamente e garanta que o computador estará limpo.

Para agendar uma verificação:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Outras configurações** > **Verificação agendada**.
3. Ative a **Verificação agendada**.
4. Selecione quando deseja que a verificação seja iniciada.

Opção	Descrição
Diariamente	Verifica o computador todos os dias.
Semanalmente	Verifica o computador em dias selecionados da semana. Selecione os dias na lista.
Mensalmente	Verifica o computador em dias selecionados do mês. Para selecionar os dias: 1. Selecione uma das opções de **Dia**. 2. Selecione o dia do mês na lista ao lado do dia selecionado.

5. Selecione quando você quer iniciar a verificação nos dias selecionados.

Opção	Descrição
Hora de início	Inicia a verificação em um momento especificado.
Depois que o computador não for usado por	Inicia a verificação após o computador estar sem uso por um período de tempo especificado.

A verificação agendada usa as configurações da verificação manual quando verifica seu computador, exceto ao verificar arquivos compactados todas as vezes e limpar arquivos perigosos automaticamente.

Verificar e-mails

A verificação de e-mails impede que você receba arquivos perigosos em e-mails enviados a você.

A verificação de vírus e spyware precisa estar ativada para verificar e-mails em busca de vírus.

Para ativar e desativar a verificação de e-mail:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Selecione **Remover anexos de e-mail perigosos**.
4. Clique em **OK**.

Quando as mensagens de e-mail e anexos são verificados

A verificação de vírus e spyware pode remover conteúdo perigoso de e-mails recebidos.

A verificação de vírus e spyware remove mensagens de e-mail perigosas recebidas por programas de e-mail como Microsoft Outlook e Outlook Express, Microsoft Mail ou Mozilla Thunderbird. Ela verifica mensagens de e-mail e anexos que não estejam criptografados toda vez que o programa de e-mails os recebe do servidor de e-mails usando protocolo POP3.

A Verificação de vírus e spyware não pode verificar mensagens de e-mail em e-mails da web, o que inclui aplicativos de e-mail executados em seu navegador da web, como Hotmail, Yahoo!Mail ou Gmail. Você ainda estará protegido de *vírus* mesmo se não remover anexos perigosos ou estiver usando e-mail da web. Quando você abre anexos de e-mails, a Verificação em tempo real remove quaisquer anexos perigosos antes que possam causar danos.

Nota: A Verificação em tempo real protege apenas seu computador, mas não seus amigos. A Verificação em tempo real não verifica arquivos anexados a menos que você abra o anexo. Isso significa que se você encaminhar uma mensagem pelo e-mail da web antes de abrir o anexo, poderá encaminhar um e-mail infectado aos seus amigos.

Ver os resultados da verificação

O histórico de vírus e spyware exibe todos os arquivos perigosos que o produto já encontrou.

Às vezes, o produto não pode realizar a ação selecionada quando algo perigoso é encontrado. Por exemplo, se você selecionar limpar os arquivos e um arquivo não puder ser limpo, o produto o moverá para a quarentena. Você pode ver estas informações no histórico de vírus e spyware.

Para ver o histórico:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Clique em **Ver histórico de remoções**.

O histórico de vírus e spyware exibe as seguintes informações:

- data e hora em que um arquivo perigoso foi encontrado,
- nome do malware e sua localização no computador e
- a ação realizada.

Como excluir arquivos da verificação

Talvez você queira excluir alguns arquivos ou aplicativos da verificação. Itens excluídos não são verificados a menos que você os remova da lista de itens excluídos.

Nota: Listas de exclusão são separadas para verificação em tempo real e verificação manual. Por exemplo, se você excluir um arquivo da verificação em tempo real, ele será verificado durante a verificação manual exceto se você também excluí-lo da verificação manual.

Excluir tipos de arquivo

Quando você exclui arquivos por seu tipo, arquivos com extensões específicas não são verificados em busca de conteúdo perigoso.

Para adicionar ou remover o tipo de arquivo que deseja excluir da verificação:

1. Na página principal, clique em **Configurações**.

Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Escolha se deseja excluir o tipo de arquivo da verificação manual ou em tempo real:
   - Selecione **Computer Security** > **Verificação de vírus e spyware** para excluir o tipo de arquivo da verificação em tempo real.
   - Selecione **Outras configurações** > **Verificação manual** para excluir o tipo de arquivo da verificação manual.
3. Clique em **Excluir arquivos da verificação**.
4. Para excluir um tipo de arquivo:
   a) Selecione a guia **Tipos de Arquivo**.
   b) Selecione **Excluir arquivos com estas extensões**.
   c) Digite uma extensão de arquivo que identifique o tipo de arquivo que você deseja excluir no campo próximo ao botão **Adicionar**.

      Para especificar arquivos que não têm extensão, digite ".". Você pode usar o coringa "?" para representar qualquer caractere único ou "'*" para representar qualquer número de caracteres.

      Por exemplo, para excluir arquivos executáveis, digite `exe` no campo.
   d) Clique em **Adicionar**.
5. Repita a etapa anterior para excluir qualquer outra extensão da verificação de vírus.
6. Clique em **OK** para fechar a caixa de diálogo **Excluir da Verificação**.
7. Clique em **OK** para aplicar as novas configurações.

Os tipos de arquivos selecionados são excluídos das verificações futuras.

Excluir arquivos de acordo com o local

Quando você exclui arquivos por local, arquivos em unidades ou pastas especificadas não são verificados em busca de conteúdo perigoso.

Para adicionar ou remover locais com arquivos que deseja excluir da verificação:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.
2. Escolha se deseja excluir o local da verificação manual ou em tempo real:
   - Selecione **Computador** > **Verificação de vírus e spyware** para excluir o local da verificação em tempo real.
   - Selecione **Computador** > **Verificação manual** para excluir o local da verificação manual.
3. Clique em **Excluir arquivos da verificação**.
4. Para excluir um arquivo, unidade ou pasta:
   a) Selecione a guia **Objetos**.
   b) Selecione **Excluir objetos (arquivos, pastas, ...)**.
   c) Clique em **Adicionar**.
   d) Selecione o arquivo, unidade ou pasta a ser excluído da verificação em busca de vírus.

      Nota: Algumas unidades podem ser removíveis, como CD, DVD, ou unidades de rede. Unidades de rede e unidades removíveis vazias não podem ser excluídas.

   e) Clique em **OK**.
5. Repita a etapa anterior para excluir outros arquivos, unidades ou pastas da verificação contra vírus.
6. Clique em **OK** para fechar a caixa de diálogo **Excluir da Verificação**.

7. Clique em **OK** para aplicar as novas configurações.

Os arquivos, unidades ou pastas selecionados são excluídos das verificações futuras.

Ver aplicativos excluídos

Você pode ver os aplicativos que excluiu da verificação e removê-los da lista de itens excluídos se desejar que sejam verificados no futuro.

Se a verificação manual ou em tempo real detectar um aplicativo que se comporta como spyware ou riskware mas você sabe que é seguro, é possível excluí-lo da verificação para que o produto não avise mais você sobre esse aplicativo.

Nota: Se o aplicativo se comportar como um vírus ou outro software malicioso, não poderá ser excluído da verificação.

Não é possível excluir arquivos da verificação diretamente. Novos aplicativos aparecem na lista de exclusão apenas se você os excluir durante a verificação.

Para ver os aplicativos que foram excluídos da verificação:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Escolha se deseja ver os aplicativos que foram excluídos da verificação manual ou da verificação em tempo real:
   - Selecione **Computador** > **Verificação de vírus e spyware** para ver os aplicativos que foram excluídos da verificação em tempo real.
   - Selecione **Computador** > **Verificação manual** para ver os aplicativos que foram excluídos da verificação manual.
3. Clique em **Excluir arquivos da verificação**.
4. Selecione a guia **Aplicativos**.

   Nota: Apenas aplicativos de spyware e riskware podem ser excluídos, não vírus.

5. Se desejar verificar o aplicativo excluído da verificação novamente:
   a) Selecione o aplicativo que deseja incluir na verificação.
   b) Clique em **Remover**.
6. Clique em **OK** para fechar a caixa de diálogo **Excluir da Verificação**.
7. Clique em **OK** para sair.

Como utilizar a quarentena

A quarentena é um repositório seguro para arquivos que podem ser perigosos.

Os arquivos em quarentena não conseguem se espalhar ou causar qualquer dano ao seu computador.

Você pode colocar *malwares*, *spywares* e *riskwares* em quarentena para impedir que causem danos. Se necessário, também é possível restaurar aplicativos ou arquivos da quarentena posteriormente.

Se você não precisar de um item em quarentena, pode exclui-lo. A exclusão de um item da quarentena remove-o permanentemente do computador.

- Em geral, é possível excluir um *malware* que está em quarentena.

- Na maioria das vezes, você pode excluir o *spyware* que está em quarentena. É possível que o *spyware* em quarentena faça parte de um programa legítimo e a sua remoção poderá impedir o programa de funcionar corretamente. Para manter o programa no computador, você pode restaurar o *spyware* que está em quarentena.
- Um *riskware* que está em quarentena pode ser um programa legítimo. Se você mesmo instalou e configurou o programa, poderá restaurá-lo da quarentena. Se o *riskware* foi instalado sem o seu conhecimento, é muito provável que tenha sido instalado com intenções maliciosas e deverá ser excluído.

Ver itens em quarentena

Você pode ver mais informações sobre os itens em quarentena.

Para ver informações detalhadas sobre os itens em quarentena:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Clique em **Ver quarentena**.
   A página **Quarentena** mostra o número total de itens armazenados na quarentena.
4. Para ver informações detalhadas sobre a quarentena, clique em **Detalhes**.

   Você pode classificar o conteúdo por caminho do arquivo ou nome do malware.

   Uma lista dos primeiros 100 itens é mostrada com o tipo dos itens em quarentena, nome e caminho onde os arquivos foram instalados.
5. Para ver mais informações sobre um item em quarentena, clique no ícone ao lado do item na coluna **Estado**.

Restaurar itens da quarentena

É possível restaurar os itens da quarentena, se for necessário.

É possível restaurar aplicativos ou arquivos da quarentena se for necessário. Não restaure itens da quarentena a menos que você tenha certeza de que não podem causar danos. Os itens restaurados são colocados de volta no local original no seu computador.

Para restaurar itens da quarentena:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **Verificação de vírus e spyware**.
3. Clique em **Ver quarentena**.
4. Selecione os itens em quarentena que deseja restaurar.
5. Clique em **Restaurar**.

O que é o DeepGuard

O DeepGuard analisa o conteúdo de arquivos e o comportamento de aplicativos, além de monitorar aplicativos que não são considerados confiáveis.

O DeepGuard bloqueia *vírus* e *worms* novos e desconhecidos, e outros aplicativos perigosos que tentam fazer alterações em seu computador, além de evitar que aplicativos suspeitos acessem a internet.

Quando o DeepGuard detecta um novo aplicativo tentando fazer alterações potencialmente perigosas no sistema, ele permite que o aplicativo seja executado em uma zona segura. Na zona segura, o aplicativo não pode prejudicar seu computador. O DeepGuard analisa quais alterações o aplicativo tentou fazer e, com base nisso, decide qual é a probabilidade do aplicativo ser um *malware*. Se o aplicativo provavelmente for um *malware*, o DeepGuard o bloqueia.

Alterações potencialmente perigosas no sistema que o DeepGuard detecta incluem:

- alterações na configuração do sistema (Registro do Windows),
- tentativas de desativar programas de sistema importantes, por exemplo, os programas de segurança como este produto e
- tentativas de editar os arquivos de sistema importantes.

Ative ou desative o DeepGuard

Mantenha o DeepGuard ativado para evitar que aplicativos suspeitos façam alterações potencialmente perigosas no sistema de seu computador.

Se você tiver o Windows XP, certifique-se de instalar o Service Pack 2 antes de ativar o DeepGuard.

Para ativar ou desativar o DeepGuard:

1. Na página principal, clique em **Status**.
2. Clique em **Alterar configurações nesta página**.

   Nota: Você precisa de direitos de administrador para desativar os recursos de segurança.

3. Ative ou desative o **DeepGuard**.
4. Clique em **Fechar**.

Permitir aplicativos que o DeepGuard bloqueou

Você pode controlar quais aplicativos o DeepGuard permite e bloqueia.

Às vezes o DeepGuard pode evitar que um aplicativo seguro seja executado, mesmo se você quiser usar o aplicativo e souber que é seguro. Isso acontece porque o aplicativo tenta fazer alterações no sistema que podem ser potencialmente perigosas. Você também pode ter bloqueado o aplicativo sem intenção quando uma janela pop-up do DeepGuard foi mostrada.

Para permitir um aplicativo que o DeepGuard bloqueou:

1. Na página principal, clique em **Ferramentas**.
2. Clique em **Aplicativos**.
   A lista **Aplicativos monitorados** é exibida.
3. Encontre o aplicativo que deseja permitir.

   Nota: Você pode clicar nos cabeçalhos da coluna para organizar a lista. Por exemplo, clique na coluna **Permissão** para organizar a lista em grupos de programas permitidos e negados.

4. Selecione **Permitir** na coluna **Permissão**.
5. Clique em **Fechar**.

O DeepGuard permite que o aplicativo faça alterações no sistema novamente.

Usar o DeepGuard no modo de compatibilidade

Para obter proteção máxima, o DeepGuard modifica temporariamente programas em execução. Alguns programas verificam que não estão corrompidos ou modificados e não podem ser compatíveis com este

recurso. Poe exemplo, jogos on-line com ferramentas antitrapaça verificam que não foram modificados de nenhuma maneira quando são executados. Neste caso, você pode ativar o modo de compatibilidade.

Para ativar o modo de compatibilidade:

1. Na página principal, clique em **Configurações**.

   Nota: Você precisa de direitos de administrador para alterar as configurações.

2. Selecione **Computer Security** > **DeepGuard**.
3. Selecione **Usar o modo de compatibilidade**.
4. Clique em **OK**.

O que fazer com avisos de comportamento suspeito

O DeepGuard monitora aplicativos que não são considerados confiáveis. Se um aplicativo monitorado tenta acessar a internet, tenta fazer alterações no sistema ou se comporta de maneira suspeita, o DeepGuard o bloqueia.

Quando você seleciona **Avisar sobre comportamento suspeito** nas configurações do DeepGuard, o DeepGuard notifica você quando detecta um aplicativo potencialmente perigoso ou quando você inicia um aplicativo que tem uma reputação desconhecida.

Para decidir o que deseja fazer com o aplicativo que o DeepGuard bloqueou:

1. Clique em **Detalhes** para ver mais informações sobre o programa.
   A seção de detalhes mostra a você:
   - o local do aplicativo,
   - a reputação do aplicativo na Rede de proteção em tempo real e
   - quão comum é o aplicativo.
2. Decida se confia no aplicativo que o DeepGuard bloqueou:
   - Escolha **Confio no aplicativo. Permitir que continue.** se não quiser bloquear o aplicativo.

     O aplicativo tem maior probabilidade de ser seguro se:

     - O DeepGuard tiver bloqueado o aplicativo como resultado de algo que você fez,
     - você reconhecer o aplicativo ou
     - você tiver obtido o aplicativo de uma fonte segura.
   - Escolha **Não confio no aplicativo. Mantê-lo bloqueado.** se desejar manter o aplicativo bloqueado.

     O aplicativo tem maior probabilidade de não ser seguro se:

     - o aplicativo não for comum,
     - o aplicativo tiver uma reputação desconhecida ou
     - você não conhecer o aplicativo.
3. Se você desejar enviar um aplicativo suspeito para análise:
   a) Clique em **Denunciar o aplicativo para a F-Secure**.
   O produto exibe as condições de envio.
   b) Clique em **Aceito** se concordar com as condições e desejar enviar a amostra.

   Recomendamos que você envie uma amostra quando:

   - O DeepGuard bloquear um aplicativo que você sabe que é seguro ou
   - você suspeitar que o aplicativo pode ser um *malware*.