F-Secure Anti-Virus 2013

Conteúdos

Capítulo 1: Instalação.....5

Antes de instalar a aplicação pela primeira vez.....6
Instalar o produto pela primeira vez.....6
Instalar e actualizar aplicações.....6
Ajuda e Assistência.....7

Capítulo 2: Introdução.....9

Como utilizar actualizações automáticas.....10
Verificar o estado da actualização.....10
Alterar as minhas definições de ligação à Internet.....10
Verifique o estado da Rede de protecção em tempo real.....11
Como visualizar as acções efectuadas pelo produto.....11
Visualizar histórico de notificações.....11
Alterar as definições de notificação.....11
Rede de protecção em tempo real.....12
O que é a Rede de protecção em tempo real.....12
Vantagens da Rede de protecção em tempo real.....12
Com que dados contribui.....13
Como protegemos a sua privacidade.....14
Tornar-se um contribuidor para a Rede de protecção em tempo real.....14
Questões acerca da Rede de protecção em tempo real.....15
Como saber se a minha subscrição é válida.....15
Centro de acções.....16
Activar uma subscrição.....16

Capítulo 3: Introdução.....17

Visualizar o estado geral da minha protecção.....18
Visualizar as estatísticas do produto.....18
Tratar as actualizações do produto.....19
Visualizar versões da base de dados.....19
Alterar as definições da banda larga móvel.....19
O que são vírus e outro malware.....20
Vírus.....20
Spyware.....21
Rootkits.....21
Riskware.....21

Capítulo 4: Proteger o meu computador contra malware.....23
Como analisar o meu computador.....24
Analisar os ficheiros manualmente.....24
Analisar os ficheiros manualmente.....26
Analisar mensagens de correio electrónico.....29
Visualizar os resultados da análise.....30
Como excluir ficheiros da análise.....30
Excluir tipos de ficheiro.....30
Excluir ficheiros por localização.....31
Ver aplicações excluídas.....32
Como utilizar a quarentena.....32
Ver itens em quarentena.....33
Restaurar itens em quarentena.....33
O que é o DeepGuard.....33
Activar ou desactivar a aplicação DeepGuard.....34
Permitir aplicações que a aplicação DeepGuard tenha bloqueado.....34
Utilize a aplicação DeepGuard no modo de compatibilidade.....34
O que fazer com avisos de comportamentos suspeitos.....35

Capítulo

1

Instalação

Tópicos:

- *Antes de instalar a aplicação pela primeira vez*
- *Instalar o produto pela primeira vez*
- *Instalar e actualizar aplicações*
- *Ajuda e Assistência*

Antes de instalar a aplicação pela primeira vez

Obrigado por ter escolhido a F-Secure.

Para instalar o produto, precisa do seguinte:

- O CD de instalação ou um pacote de instalação. Se estiver a utilizar um netbook sem uma unidade de CD, pode transferir o pacote de instalação a partir de *www.f-secure.com/netbook*.
- A sua chave de subscrição.
- Uma ligação à Internet.

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

Nota: Se tiver mais de uma conta no computador, inicie sessão com privilégios de administrador durante a instalação.

Instalar o produto pela primeira vez

Instruções para instalar o produto.

Siga estas instruções para instalar o produto:

1. Introduza o CD ou faça duplo clique no instalador que transferiu.

   Se o CD não arrancar automaticamente, vá até ao Explorador do Windows, faça duplo clique no ícone de CD-ROM e faça duplo clique no ficheiro de instalação para iniciar a instalação.

2. Siga as instruções no ecrã.

   - Se tiver adquirido o produto em formato de CD numa loja, pode encontrar a chave de subscrição na capa do Guia de instalação rápida.
   - Se tiver transferido o produto a partir da F-Secure eStore, a chave de subscrição está incluída na mensagem de correio electrónico de confirmação da ordem de encomenda.

   Pode ser necessário reiniciar o computador antes de validar a subscrição e transferir as actualizações mais recentes a partir da Internet. Se estiver a efectuar a instalação a partir de um CD, lembre-se de retirar o CD de instalação antes de reiniciar o computador.

Instalar e actualizar aplicações

Instruções para activar a nova subscrição.

Siga estas instruções para activar a nova subscrição ou para instalar uma nova aplicação utilizando o painel de iniciação:

Nota: Pode encontrar o ícone do painel de iniciação no tabuleiro de sistema do Windows.

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Visualizar as minhas subscrições**
3. Em **As minhas subscrições**, vá até à página **Estado da subscrição** e clique em **Activar subscrição**.
   É aberta a janela **Activar subscrição**.

4. Introduza a chave de subscrição para a aplicação e clique em **OK**.
5. Depois da validação e activação da subscrição, clique em **Fechar**.
6. Em **As minhas subscrições**, vá até à página **Estado da instalação**. Se a instalação não começar automaticamente, siga estas instruções:
   a) Clique em **Instalar**.
   É aberta a janela de instalação.
   b) Clique em **Seguinte**.
   A aplicação é transferida e é iniciada a instalação.
   c) Quando a instalação estiver concluída, clique em **Fechar**.

A nova subscrição foi activada.

Ajuda e Assistência

Pode aceder à ajuda online do produto ao clicar no ícone de Ajuda ou premindo F1 em qualquer ecrã do produto.

Depois de registar a licença, tem direito a serviços adicionais como actualizações gratuitas do produto e assistência do produto. Pode efectuar o registo em *www.f-secure.com/register*.

Capítulo

2

Introdução

Tópicos:

- *Como utilizar actualizações automáticas*
- *Como visualizar as acções efectuadas pelo produto*
- *Rede de protecção em tempo real*
- *Como saber se a minha subscrição é válida*

Informações acerca de como começar a utilizar o produto.

Esta secção descreve como alterar as definições comuns e gerir as subscrições através do painel de iniciação.

As definições comuns do painel de iniciação são definições aplicáveis a todos os programas instalados no painel de iniciação. Em vez de alterar as definições em separado em cada programa, pode simplesmente editar as definições comuns, que serão então utilizadas por todos os programas instalados.

As definições comuns do painel de iniciação incluem:

- Transferências, onde pode visualizar informações acerca das actualizações que têm sido transferidas e verificar manualmente se estão disponíveis novas actualizações.
- Definições de ligação, onde pode alterar a forma como o computador estabelece ligação à Internet.
- Notificações, onde pode visualizar notificações anteriores e visualizar o tipo de notificações que desejar.
- Definições de privacidade, onde pode seleccionar se o computador tem ou não permissão para estabelecer ligação à Rede de protecção em tempo real.

Também pode gerir as subscrições para os programas instalados através do painel de iniciação.

Como utilizar actualizações automáticas

As actualizações automáticas mantêm a protecção do seu computador actualizada.

O produto transfere as actualizações mais recentes para o seu computador, quando se liga à Internet. Detecta o tráfego da rede e não prejudica outros processos com ligação à Internet, mesmo quando a ligação é lenta.

Verificar o estado da actualização

Ver data e hora da última actualização.

Quando as actualizações automáticas estão activadas, o produto recebe as actualizações mais recentes automaticamente quando existe uma ligação à Internet.

Para ter a certeza de que tem as actualizações mais recentes:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Abrir definições comuns**.
3. Seleccione **Actualizações automáticas** > **Transferências**.
4. Clique em **Verificar**.
   O produto liga-se à Internet e procura as actualizações mais recentes.Se a protecção não estiver actualizada, transfere as últimas actualizações.

   Nota: Se estiver a utilizar um modem ou uma ligação RDIS para ligar à Internet, a ligação terá de estar activa para que o programa verifique se existem actualizações.

Alterar as minhas definições de ligação à Internet

Normalmente não existe necessidade de alterar as definições predefinidas mas pode configurar a forma como o servidor estabelece a ligação à Internet de forma a poder receber actualizações automaticamente.

Para alterar as definições de ligação à Internet:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Abrir definições comuns**.
3. Seleccione **Actualizações automáticas** > **Ligação**.
4. Em **Ligação à Internet** na lista, seleccione a forma como o computador estabelece ligação à Internet.
   - Seleccione **Pressupor sempre que está ligado** se tiver uma ligação de rede permanente.

     Nota: Se o seu computador não utilizar uma ligação permanente, mas sim uma ligação telefónica, seleccionar **Pressupor sempre que está conectado** pode fazer com que o telefone esteja sempre a marcar a ligação.
   - Seleccione **Detectar conexão** para transferir actualizações só quando o produto detectar uma ligação activa.
   - Seleccione **Detectar tráfego** para transferir actualizações só quando o produto detectar tráfego de outra rede.

     Dica: Se tiver uma configuração de hardware fora do comum, que obrigue a definição **Detectar conexão** a detectar uma ligação activa mesmo que não exista nenhuma, seleccione **Detectar tráfego**.

5. Na lista **HTTP proxy**, seleccione se o computador utiliza ou não um *servidor proxy* para estabelecer ligação à Internet.
   - Seleccione**Sem HTTP proxy** se o computador estiver ligado à Internet directamente.
   - Seleccione **Configurar manualmente o proxy HTTP** para configurar as definições *Proxy HTTP*.
   - Seleccione **Utilizar o proxy HTTP do meu explorador** para utilizar as mesmas definições do *proxy HTTP* que configurou para o explorador de Internet.

Verifique o estado da Rede de protecção em tempo real

Para funcionar de forma adequada, muitas funcionalidades do produto dependem da ligação da Rede de protecção em tempo real.

Se existirem problemas de rede ou se a firewall bloquear o tráfego da Rede de protecção em tempo real, o estado é 'desligada'. Se não estiverem instaladas funcionalidades que necessitem de acesso à Rede de protecção em tempo real, o estado é 'não está a ser utilizada'.

Para verificar o estado:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Abrir definições comuns**.
3. Seleccione **Actualizações automáticas** > **Ligação**.

Em **Rede de protecção em tempo real**, pode visualizar o estado actual da Rede de protecção em tempo real.

Como visualizar as acções efectuadas pelo produto

Pode visualizar as acções efectuadas pelo computador na página **Notificações**.

O produto irá apresentar uma notificação quando efectuar uma acção, por exemplo quando encontrar e bloquear um vírus. Algumas notificações também podem ser enviadas pelo seu fornecedor de serviço, por exemplo para o informar acerca de novos serviços disponíveis.

Visualizar histórico de notificações

Pode visualizar as notificações que foram apresentadas no histórico de notificações

Para visualizar o histórico de notificações:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Abrir definições comuns**.
3. Seleccione **Outros** > **Notificações**.
4. Clique em **Mostrar histórico de notificações**.
   É aberta a lista de histórico de notificações.

Alterar as definições de notificação

Pode seleccionar o tipo de notificações que deseja que sejam apresentadas pelo produto.

Para alterar as definições de notificação:

1. No painel de iniciação, clique com o botão direito do rato no ícone.

É apresentado um menu pendente.

2. Seleccione **Abrir definições comuns**.
3. Seleccione **Outros** > **Notificações**.
4. Seleccione ou anule a selecção de **Permitir mensagens do programa** para activar ou desactivar as mensagens do programa.

   Quando a definição é activada, o produto apresenta notificações para os programas instalados.
5. Seleccione ou anule a selecção de **Permitir mensagens promocionais** para activar ou desactivar as mensagens promocionais.
6. Clique em **OK**.

Rede de protecção em tempo real

Este documento descreve a Rede de protecção em tempo real, um serviço online da F-Secure Corporation que identifica aplicações e páginas da Internet limpas e oferece protecção contra malware e exploradores de páginas da Internet.

O que é a Rede de protecção em tempo real

A Rede de protecção em tempo real é um serviço online que oferece uma resposta rápida contra as ameaças mais recentes baseadas na Internet.

Como contribuidor para a Rede de protecção em tempo real, pode ajudar-nos a fortalecer a protecção contra ameaças novas e emergentes. A Rede de protecção em tempo real recolhe estatísticas de determinadas aplicações desconhecidas, maliciosas ou suspeitas e acerca de como se comportam no dispositivo. Estas informações são anónimas e enviadas para a F-Secure Corporation para análise de dados combinados. Utilizamos as informações analisadas para melhorar a segurança no dispositivo contra as ameaças mais recentes e ficheiros maliciosos.

Como funciona a Rede de protecção em tempo real

Como contribuidor para a Rede de protecção em tempo real, pode fornecer informações acerca de aplicações e páginas da Internet desconhecidas e acerca de aplicações maliciosas e explorações em páginas da Internet. A Rede de protecção em tempo real não rastreia a sua actividade na internet nem recolhe informações acerca das páginas da Internet que já foram analisadas e não recolhe informações acerca de aplicações fidedignas instaladas no computador.

Se não desejar contribuir com estes dados, a Rede de protecção em temo real não recolhe informações acera das aplicações instaladas ou páginas da Internet visitadas. No entanto, o produto precisa de questionar os servidores da F-Secure acerca da reputação das aplicações, páginas da Internet, mensagens e outros assuntos. A questão é colocada utilizando uma soma de verificação encriptada na qual o próprio assunto questionado não é enviado para a F-Secure. Não rastreamos dados por utilizador, apenas se a contagem de ocorrências do ficheiro ou da página da Internet está a aumentar.

Não é possível interromper por completo todo o tráfego de rede para a Rede de protecção em tempo real, uma vez que é parte integrante da protecção fornecida pelo produto.

Vantagens da Rede de protecção em tempo real

Com a Rede de protecção em tempo real, terá uma protecção mais rápida e precisa contra as ameaças mais recentes e não irá receber alertas desnecessários para aplicações suspeitas que não são maliciosas.

Como contribuidor para a Rede de protecção em tempo real, pode ajudar-nos a detectar malware novo e não detectado e eliminar possíveis falsos positivos da nossa base de dados de definição de vírus.

Todos os participantes na Rede de protecção em tempo real se ajudam entre si. Quando a Rede de protecção em tempo real detecta uma aplicação suspeita no seu dispositivo, beneficia dos resultados da análise quando a mesma aplicação já tiver sido encontrada noutros dispositivos. A Rede de protecção em tempo real melhora o desempenho global do seu dispositivo, uma vez que o produto de segurança instalado não necessita de analisar novamente as aplicações que a Rede de protecção em tempo real já tenha analisado e concluído como estando limpas. Da mesma forma, as informações acerca de páginas da Internet maliciosas e mensagens publicitárias não solicitadas são partilhadas através da Rede de protecção em tempo real e podemos fornecer-lhe uma protecção mais precisa contra exploradores em páginas da Internet e mensagens de Spam.

Quanto mais pessoas contribuírem para a Rede de protecção em tempo real, mais bem protegidos estarão os participantes individuais.

Com que dados contribui

Como contribuidor para a Red de protecção em tempo real, fornece informações acerca de aplicações armazenadas no dispositivo e nas páginas da Internet que visita, de forma a que a Rede de protecção em tempo real possa oferecer protecção contra as aplicações maliciosas mais recentes e páginas da Internet suspeitas.

Analisar a reputação dos ficheiros

A Rede de protecção em tempo real apenas recolhe informações acerca das aplicações que não possuem uma reputação reconhecida e acerca de ficheiros suspeitos ou conhecidos por serem malware.

A Rede de protecção em tempo real recolhe informações anónimas acerca de aplicações limpas ou suspeitas no dispositivo. A Rede de protecção em tempo real reacolhe informações apenas acerca de ficheiros executáveis (como os ficheiros executáveis portáteis na plataforma Windows, com extensões de ficheiros .cpl, .exe, .dll, .ocx, .sys, .scr e .drv).

As informações recolhidas incluem:

- o caminho do ficheiro no qual se encontra a aplicação no dispositivo,
- o tamanho do ficheiro e a data de criação ou modificação,
- atributos e privilégios do ficheiro,
- as informações da assinatura do ficheiro,
- a versão actual do ficheiro e a empresa que o criou,
- a origem do ficheiro ou o respectivo URL de transferência e
- Os resultados da análise antivírus e da aplicação F-Secure DeepGuard dos ficheiros analisados e
- outras informações similares.

A Rede de protecção em tempo real nunca recolhe quaisquer informações acerca dos seus documentos pessoais, a menos que os mesmos estejam infectados. Para qualquer tipo de ficheiro malicioso, recolhe o nome da infecção e o estado de desinfecção do ficheiro.

Com a Rede de protecção em tempo real, também pode enviar aplicações suspeitas para análise. As aplicações que envia incluem apenas ficheiros executáveis portáteis. A Rede de protecção em tempo real nunca recolhe informações acerca dos seus documentos pessoais e nunca são carregados automaticamente para análise.

Enviar ficheiros para análise

Com a Rede de protecção em tempo real, também pode enviar aplicações suspeitas para análise.

Pode enviar aplicações suspeitas individuais manualmente quando o produto assim o solicitar. Apenas pode enviar ficheiros Executáveis Portáteis. A Rede de protecção em tempo real nunca transfere os seus documentos pessoais.

Analisar a reputação da página da Internet

A Rede de protecção em tempo real não regista a sua actividade na Internet nem recolhe informações acerca das páginas da Internet que já tenham sido analisadas. Garante que as páginas da Internet visitas são seguras à medida que navega na Internet, A Rede de protecção em tempo real verifica a segurança das páginas e notifica-o se a página estiver classificada como suspeita ou nociva.

Se a página da Internet que visitar contiver conteúdos maliciosos ou suspeitos ou um explorador conhecido, a Rede de protecção em tempo real recolhe o URL completo da página para que o conteúdo da página da Internet possa ser analisado.

Se visitar uma página que ainda não tenha sido classificada, a Rede de protecção em tempo real recolhe os nomes do domínio e do subdomínio e, em alguns casos, o caminho para a página visitada, para que a página possa ser analisada e classificada. Todos os parametros do URL que possam conter informações que possam ser ligadas a si num formato identificável pessoalmente são removidos para proteger a sua privacidade.

Nota: A Rede de protecção em tempo real não classifica nem analisa páginas da Internet em redes privadas, pelo que nunca recolhe quaisquer informações acerca de endereços IP privados (por exemplo, redes internas empresariais).

Analisar as informações do sistema

A Rede de protecção em tempo real recolhe o nome e a versão do sistema operativo, informações acerca da ligação à Internet e as estatísticas de utilização da Rede de protecção em tempo real (por exemplo, o número de vezes que foi questionada a reputação de uma página da Internet e o intervalo médio de tempo para apresentar um resultado) para que possamos monitorizar e melhorar o serviço.

Como protegemos a sua privacidade

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

A Rede de protecção em tempo real elimina os dados identificativos antes de os enviar para a F-Secure e encripta todas as informações recolhidas durante a transferência para os proteger de acessos não autorizados. As informações recolhidas não são processadas individualmente, são agrupadas com informações de outros contribuidores para a Rede de protecção em tempo real. Todos os dados são analisados estatisticamente de forma anónima, o que significa que não será estabelecida de forma alguma a relação entre si e os dados.

Quaisquer informações que o possam identificar individualmente não são incluídas nos dados recolhidos. A Rede de protecção em tempo real não recolhe endereços IP privados ou as suas informações pessoais, como endereços de correio electrónico, nomes de utilizador e palavras-passe. Apesar de encetarmos todos os esforços para remover todos os dados identificáveis a nível pessoal, é possível que alguns dados identificáveis permaneçam nas informações recolhidas. Nesses casos, não procuraremos utilizar de forma não intencional dados recolhidos para o identificar.

Aplicamos medidas de segurança e protecções técnicas, administrativas e físicas estritas para proteger as informações recolhidas durante a transferência, armazenamento e processamento das mesmas. As informações são armazenadas em locais seguros e em servidores que são controlados nos nossos escritórios ou nos escritórios das empresas por nós contratadas. Apenas pessoal autorizado pode aceder às informações recolhidas.

A F-Secure pode partilhar os dados recolhidos com as suas filiadas, sub-contratadas, distribuidores e parceiros mas sempre num formato anónimo e não identificável.

Tornar-se um contribuidor para a Rede de protecção em tempo real

Ajuda-nos a melhorar a Rede de protecção em tempo real ao contribuir com informações acerca de programas e páginas da Internet maliciosos.

Pode escolher participar na Rede de protecção em tempo real durante a instalação. Com as definições predefinidas de instalação, contribui com dados para a Rede de protecção em tempo real. Pode alterar esta definição mais tarde no produto.

Siga estas instruções para alterar as definições da Rede de protecção em tempo real:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Abrir definições comuns**.
3. Seleccione **Outros** > **Privacidade**.
4. Seleccione a caixa de verificação de participação para se tornar um contribuidor para a Rede de protecção em tempo real.

Questões acerca da Rede de protecção em tempo real

Informações de contacto para quaisquer questões acerca da Rede de protecção em tempo real.

Se tiver quaisquer questões adicionais acerca da Rede de protecção em tempo real, contacte:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsínquia

Finlândia

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

A versão mais recente desta política está sempre disponível na nossa página na Internet.

Como saber se a minha subscrição é válida

O tipo e o estado da subscrição são apresentados na página **Estado da subscrição**.

Quando a subscrição estiver prestes a expirar, ou se tiver expirado, o estado de protecção geral do programa no ícone correspondente no painel de iniciação é alterado.

Para verificar a validade da sua subscrição:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Visualizar as minhas subscrições**.
3. Seleccione **Estado da subscrição** para visualizar informações acerca das subscrições dos programas instalados.
4. Seleccione **Estado da instalação** para visualizar os programas disponíveis para serem instalados.

O estado da subscrição e a data de validade também são apresentados na página **Estatísticas** do programa. Se a subscrição tiver expirado, deve renovar a subscrição para continuar a receber actualizações e utilizar o produto.

Nota: Quando a subscrição tiver expirado, o ícone de estado do produto fica intermitente no tabuleiro do sistema.

Centro de acções

O Centro de acções apresenta-lhe quaisquer notificações importantes que exijam a sua atenção.

Se a subscrição tiver expirado ou estiver prestes a expirar, o Centro de acções notifica-o. A cor do fundo e os conteúdos do Centro de acções dependem do tipo e do estado da subscrição:

- Se a subscrição estiver prestes a expirar e, se existirem subscrições livres disponíveis, a mensagem possui uma cor de fundo branca e um botão **Activar**.
- Se a subscrição estiver prestes a expirar e não existirem subscrições livres disponíveis, a mensagem possui uma cor de fundo amarela e os botões **Comprar** e **Introduzir chave**. Se já tiver adquirido uma nova subscrição, pode clicar em **Introduzir chave** para indicar a chave de subscrição e activar a nova subscrição.
- Se a subscrição tiver expirado e existirem subscrições livres disponíveis, a mensagem possui uma cor de fundo vermelha e um botão **Activar**.
- Se a subscrição tiver expirado e não existirem subscrições livres disponíveis, a mensagem possui uma cor de fundo vermelha e os botões **Comprar** e **Introduzir chave**. Se já tiver adquirido uma nova subscrição, pode clicar em **Introduzir chave** para indicar a chave de subscrição e activar a nova subscrição.

Nota: A hiperligação **Mostrar histórico de notificações** no Centro de acções apresenta uma lista de mensagens de notificação do produto, não as mensagens anteriores do Centro de acções.

Activar uma subscrição

Quando tiver uma nova chave de subscrição ou um novo código de campanha para um produto, deve proceder à activação do mesmo.

Para activar uma subscrição:

1. No painel de iniciação, clique com o botão direito do rato no ícone.
   É apresentado um menu pendente.
2. Seleccione **Visualizar as minhas subscrições**.
3. Escolha uma das seguintes opções:
   - Clique em **Activar subscrição**.
   - Clique em **Activar código de campanha**.
4. Na caixa de diálogo que é aberta, introduza a nova chave de subscrição ou código de campanha e clique em **OK**.

   Dica: Se tiver recebido a chave de subscrição através de correio electrónico, pode copiar a chave a partir da mensagem e colar a chave no campo.

Depois de introduzir a nova chave de subscrição, A nova data de validade da subscrição é apresentada na página **Estado da subscrição**.

Capítulo

3

Introdução

Tópicos:

- *Visualizar o estado geral da minha protecção*
- *Visualizar as estatísticas do produto*
- *Tratar as actualizações do produto*
- *O que são vírus e outro malware*

Este produto protege o computador de vírus e outras aplicações nocivas.

O produto analisa ficheiros e aplicações e é actualizado automaticamente. Não requer quaisquer acções da sua parte.

Visualizar o estado geral da minha protecção

A página **Estado** apresenta-lhe um breve resumo das funcionalidades do produto instalado e o respectivo estado actual.

Para abrir a página **Estado**:

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

É aberta a página **Estado**.

Os ícones apresentam-lhe o estado do programa e as respectivas funcionalidades de segurança.

Ícone de estado	Nome do estado	Descrição
	OK	O computador está protegido. A funcionalidade está activa e a funcionar correctamente.
	Informações	O produto informa-o acerca de um estado especial de uma funcionalidade. Por exemplo, a funcionalidade está a ser actualizada.
	Aviso	O computador não está totalmente protegido. Por exemplo, o produto não recebe actualizações há muito tempo ou o estado de uma funcionalidade requer atenção.
	Erro	O seu computador não está protegido Por exemplo, a subscrição expirou ou uma funcionalidade crítica está desactivada.
	Desactivado	Uma funcionalidade não crítica está desactivada.

Visualizar as estatísticas do produto

Pode visualizar as acções efectuadas pelo produto desde a sua instalação em **Estatísticas**.

Para abrir a página **Estatísticas**:

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

É aberta a página **Estatísticas**.

- A **Última verificação de actualizações bem sucedida** mostra a hora da última actualização.

- O campo **Análise de vírus e spyware** mostra quantos ficheiros foram analisados e eliminados pelo produto desde a instalação.
- **Aplicações** apresenta o número de programas que o DeepGuard permitiu ou bloqueou desde a instalação.
- **Ligações da firewall** apresenta o número de ligações permitidas e bloqueadas desde a instalação.
- **Filtros de spam e phishing** apresenta quantas mensagens de correio electrónico o produto detectou como mensagens de correio electrónico válidas e como mensagens de spam.

Tratar as actualizações do produto

O produto mantém a protecção actualizada automaticamente.

Visualizar versões da base de dados

Pode visualizar as actualizações mais recentes e os números das versões na página **Actualizações da base de dados**.

Para abrir a página **Actualizações da base de dados**:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Outras definições** > **Versões da base de dados**.

A página **Versões da base de dados** apresenta a data mais recente de actualização das definições de vírus e spyware, da aplicação DeepGuard e dos filtros de spam e phishing, assim como os respectivos números das versões.

Alterar as definições da banda larga móvel

Seleccione se deseja transferir actualizações de segurança quando utilizar banda larga móvel.

Nota: Esta funcionalidade apenas está disponível no Microsoft Windows 7.

Por predefinição, as actualizações de segurança são sempre transferidas quando estiver dentro da rede do operador. No entanto, as actualizações são suspensas quando visitar a rede de outro operador. Isto deve-se ao facto dos preços das ligações poderem variar entre operadores, por exemplo, em países diferentes. Pode considerar manter esta definição inalterada, Se desejar economizar banda larga e, possivelmente, também custos durante a sua deslocação.

Nota: Esta definição apenas é aplicável a ligações de banda larga móvel. Quando o computador estiver ligado a uma rede sem fios fixa, o produto é actualizado automaticamente.

Para alterar a definição:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Outras definições** > **Largura de banda móvel** > **Transferir actualizações de segurança**.
3. Seleccione a opção de actualização preferida para as ligações móveis:

   - **Apenas na rede do meu operador doméstico**

     As actualizações são sempre transferidas na rede do operador. Quando visitar a rede de outro operador, as actualizações são suspensas. Recomendamos que seleccione esta opção para manter o produto actualizado ao custo previsível.

- **Nunca**

  As actualizações não são transferidas quando utilizar a largura de banda móvel.
- **Sempre**

  As actualizações são sempre transferidas, independentemente da rede que estiver a utilizar. Seleccione esta opção se quiser ter a certeza de que a segurança do computador está sempre actualizada independentemente do custo das actualizações.

4. Se pretende decidir separadamente cada vez que sair da rede do operador doméstico, seleccione **Perguntar-me cada vez que sair da rede do meu operador doméstico**.

Actualizações de segurança suspensas

As actualizações de segurança podem ser suspensas quando utilizar banda larga móvel fora da rede do seu operador.

Neste caso, pode visualizar o aviso de notificação **Suspenso** no canto inferior direito do ecrã. As actualizações estão suspensas devido aos preços das ligações poderem variar entre os operadores, por exemplo, em países diferentes. Pode considerar a manutenção desta definição inalterada, se pretender economizar largura de banda e, possivelmente, também custos, durante a sua visita. No entanto, se mesmo assim pretender alterar as definições, clique na hiperligação **Alterar**.

Nota:

Esta funcionalidade apenas está disponível no Microsoft Windows 7.

O que são vírus e outro malware

Chama-se Malware a programas especificamente concebidos para prejudicar o computador, utilizar o computador para fins ilegais ou para obter ou roubar informações aos utilizadores.

O Malware pode:

- tomar o controlo do seu navegador da Internet,
- redireccionar as suas procuras,
- mostrar publicidade não desejada,
- manter um registo das páginas da Internet visitadas,
- roubar informações pessoais, tais como informações sobre a conta bancária,
- utilizar o seu computador para enviar spam e
- utilizar o seu computador para atacar outros computadores.

O malware também pode fazer com que o seu computador se torne lento e instável. Pode suspeitar da existência de *malware* se o seu computador ficar subitamente muito lento e falhar frequentemente.

Vírus

Um vírus é, normalmente, um programa que se anexa a ficheiros e se replica rapidamente, conseguindo alterar e substituir o conteúdo de outros ficheiros, com o objectivo de danificar o computador.

Um *vírus* é um programa que, normalmente, é instalado sem o seu conhecimento. Uma vez instalado, o vírus tenta replicar-se. O vírus:

- utiliza alguns dos recursos do seu computador,
- pode alterar ou danificar ficheiros no computador,
- pode utilizar o seu computador para infectar outros computadores,
- pode permitir que o computador seja utilizado para fins ilegais.

Spyware

Spyware são programas que recolhem as suas informações pessoais.

Exemplos de dados pessoais que podem ser recolhidos:

- Endereços de websites que visitou,
- endereços de e-mail do seu computador,
- palavras-passe ou
- números de cartões de crédito.

Os programas de spyware instalam-se automaticamente sem a sua permissão ou conhecimento. O spyware pode ser instalado juntamente com um prograna útil ou quando o utilizador é levado a clicar numa opção numa janela de contexto enganadora.

Rootkits

Rootkits são programas que dificultam a detecção de outro *Malware*.

Os Rootkits ocultam ficheiros e processos. Normalmente, fazem-no para ocultar actividades maliciosas no computador. Quando um Rootkit oculta *Malware* torna-se mais difícil detectar esse Malware.

Este produto possui um detector exclusivo de Rootkit, que detecta especificamente Rootkits, para evitar que *Malware* consiga esconder-se facilmente.

Riskware

O riskware não é concebido especificamente para prejudicar o computador mas poderá prejudicá-lo se não for utilizado correctamente.

O riskware não é necessariamente malware. Os programas de riskware executam algumas funções úteis mas potencialmente perigosas.

Como exemplos de alguns programas de riskware podemos encontrar:

- programas de Mensagens Instantâneas como o IRC (Internet Relay Chat),
- programas de transferência de ficheiros de um computador para outro, através da Internet,
- Programas de Telefones através da Internet, como o VoIP (*Protocolo Voice Over Internet*) .
- Software de acesso remoto, como o VNC,
- scareware, que pode alarmar e conduzir as pessoas a adquirirem software de segurança falso ou
- software concebido para contornar verificações de CD ou protecções anti-cópia.

Se tiver sido você quem instalou o programa e o tiver configurado correctamente, provavelmente não é perigoso.

Se um Riskware tiver sido instalado sem o seu conhecimento, o mais provável é que tenha sido instalado com más intenções e deve ser removido.

Capítulo

4

Proteger o meu computador contra malware

Tópicos:

- *Como analisar o meu computador*
- *Como excluir ficheiros da análise*
- *Como utilizar a quarentena*
- *O que é o DeepGuard*

A análise para detecção de vírus e spyware protege o seu computador contra programas que poderão roubar informações pessoais, danificar o computador ou utilizá-lo para fins ilegais.

Por predefinição, todos os tipos de malware são tratados de imediato quando são detectados, pelo que não podem causar danos.

Por predefinição, as análises para detectar vírus e spyware analisam as unidades de disco rígido locais, quaisquer meios amovíveis (como unidades compactas ou discos compactos) e conteúdos transferidos automaticamente. Pode defini-las para analisar também as mensagens de correio electrónico automaticamente.

A análise de vírus e spyware também vigia o computador para detectar quaisquer alterações que possam indicar a presença de *malware*. Se existir alguma alteração perigosa no sistema, por exemplo, definições do sistema ou tentativas de alterar processos importantes do sistema, a DeepGuard impede este programa de ser executado por poder tratar-se de *malware*.

Como analisar o meu computador

Quando a análise antivírus e spyware está activa, analisa o computador para detectar automaticamente ficheiros nocivos. Também pode analisar ficheiros manualmente e configurar análises programadas.

Recomendamos que mantenha a análise antivírus e spyware sempre activa. Analise os ficheiros manualmente para garantir que não existam ficheiros nocivos no computador ou se pretender analisar ficheiros que tenha excluído da análise em tempo real.

Ao configurar uma análise programada, a análise antivírus e spyware remove os ficheiros nocivos do computador em intervalos especificados.

Analisar os ficheiros manualmente

A análise em tempo real protege o seu computador porque verifica todos os ficheiros quando são acedidos e bloqueia-lhes o acesso se contiverem *malware* .

Quando o computador tenta aceder a um ficheiro, a análise em tempo real analisa o ficheiro para detectar se contém malware antes de permitir que o computador aceda ao mesmo. A análise em tempo real detecta quaisquer conteúdos nocivos, coloca o ficheiro em quarentena antes de que possa provocar qualquer dano.

A análise em tempo real afecta o desempenho do meu computador?

Normalmente, o processo de análise passa despercebido porque demora pouco tempo e utiliza poucos recursos do sistema . O tempo e os recursos utilizados pela análise em tempo real dependem, por exemplo, do conteúdo, da localização e do tipo do ficheiro.

Ficheiros que requerem mais tempo de análise:

- Ficheiros em unidades amovíveis, tais como CDs, DVDs e unidades USB portáteis.
- Ficheiros comprimidos como, por exemplo, ficheiros *.zip*ficheiros.

  Nota: Os ficheiros comprimidos não são analisados por predefinição.

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

- tem um computador que não reúne os requisitos de sistema ou
- acede a muitos ficheiros ao mesmo tempo. Por exemplo, quando abre um directório que contém muitos ficheiros que necessitam de ser analisados.

Activar ou desactivar a análise em tempo real

Manter a análise em tempo real activa para parar o *malware* antes que possa danificar o computador.

Para activar ou desactivar a análise em tempo real:

1. Na página principal, clique em **Estado**.
2. Clique em **Alterar definições nesta página**.

   Nota: Precisa de ter direitos de administrador para desactivar as funcionalidades de segurança.

3. Activar ou desactivar a **Análise antivírus e spyware**.
4. Clique em **Fechar**.

Tratar ficheiros nocivos automaticamente

A análise em tempo real pode tratar ficheiros nocivos automaticamente sem lhe colocar quaisquer questões.

Para permitir que a análise em tempo real trate ficheiros nocivos automaticamente:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Seleccione **Tratar ficheiros nocivos automaticamente**.

Se seleccionar não tratar os ficheiros nocivos automaticamente, a análise em tempo real pergunta-lhe o que pretende fazer quando for detectado um ficheiro nocivo.

Tratar spyware

A análise antivírus e spyware bloqueia o spyware imediatamente quando este tenta iniciar.

Antes de uma aplicação de spyware poder ser iniciada, o produto bloqueia a aplicação e permite-lhe decidir o que pretende fazer com a mesma.

Opte por uma das seguintes acções quando for encontrado um spyware:

Acção a aplicar	O que acontece aos itens de spyware
Processar automaticamente	Deixe o produto decidir qual a melhor acção a tomar com base no spyware que foi encontrado.
Colocar o spyware em quarentena	Mover o spyware para a quarentena, onde não pode danificar o computador.
Eliminar o spyware	Remover todos os ficheiros relacionados com o spyware do computador.
Bloquear apenas o spyware	Bloquear o acesso ao spyware mas deixá-lo no computador.
Excluir o spyware da análise	Permitir que o spyware seja executado e excluí-lo de próximas análises.

Tratar riskware

A análise antivírus e spyware bloqueia o riskware imediatamente quando este tenta iniciar.

Antes de uma aplicação de riskware poder ser iniciada, o produto bloqueia a aplicação e permite-lhe decidir o que pretende fazer com a mesma.

Opte por uma das seguintes acções quando for encontrado um riskware:

Acção a aplicar	O que acontece ao Riskware
Bloquear apenas o riskware	Bloquear o acesso ao riskware mas deixá-lo no computador.
Colocar o riskware em quarentena	Mover o riskware para a quarentena, onde não pode danificar o computador.
Eliminar o riskware	Remover todos os ficheiros relacionados com o riskware do computador.
Excluir o riskware da análise	Permitir que o riskware seja executado e excluí-lo de próximas análises.

Remover cookies de rastreio automaticamente

Ao remover as cookies de rastreio, impede que as páginas da Internet possam rastrear as páginas que visita na Internet.

As cookies de rastreio são ficheiros pequenos que permitem às páginas da Internet rastrear as páginas que visita. Siga estas instruções para manter as cookies de rastreio desactivadas no computador.

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Seleccione **Remover cookies de rastreio**.
4. Clique em **OK**.

Analisar os ficheiros manualmente

Pode analisar os ficheiros manualmente, por exemplo, quando ligar um dispositivo externo ao computador, para garantir que não contenham qualquer malware.

Iniciar a análise manual

Pode verificar todo o computador, tipo específico de *Malware* ou uma determinada localização.

Se suspeitar de um tipo de *Malware* , pode executar uma verificação apenas para esse tipo. Se suspeitar de uma determinada área do computador, pode executar uma verificação apenas nessa área. Estas verificação demoram menos tempo a concluir que uma verificação completa do computador.

Para iniciar uma verificação manualmente:

1. Na página principal, clique na seta por baixo de **Análise**.

   São apresentadas as opções de análise.

2. Seleccione o tipo de análise.

   Seleccione **Alterar as definições da análise** para optimizar a forma como a análise manual analisa o computador para detectar vírus e outras aplicações nocivas.

3. Se tiver selecionado **Seleccionar itens a analisar**, é aberta uma janela na qual pode seleccionar a localização a analisar.
   O **Assistente de Verificação** abre.

Tipos de análise

Pode analisar todo o computador, um tipo específico de Malware ou uma determinada localização.

Segue-se uma lista dos diferentes tipos de análise:

Tipo de análise	O que é analisado	Quando utilizar este tipo
Análise de vírus e spyware	Partes do computador para detecção de vírus, spyware e riskware	Este tipo de análise é muito mais rápido do que uma análise completa. Efectua a procura apenas em partes do sistema que contêm ficheiros de programas instalados. Este tipo de análise é recomendado se quiser verificar rapidamente se o computador está limpo, pois é capaz de detectar e remover eficazmente o malware activo do seu computador.
Análise completa do computador	Todo o computador (discos rígidos internos e externos) para detecção de vírus, spyware e riskware	Quando quiser ter a certeza de que não existe Malware ou Riskware no computador.Este tipo de análise é o que demora mais tempo a concluir. Combina a análise rápida de malware com a análise do disco rígido. Também procura itens que poderão ter sido ocultados por um rootkit.
Seleccione o que deseja analisar	Um ficheiro, pasta ou unidade específicos para detecção de vírus, spyware e riskware	Quando suspeitar que uma localização específica no computador pode ter malware, por exemplo, a localização contém transferências de origens

Tipo de análise	O que é analisado	Quando utilizar este tipo
		potencialmente perigosas, tais como redes ponto-a-ponto de partilha de ficheiros. O tempo que demora a análise depende do tamanho do destino que pretende analisar. A análise é concluída rapidamente se, por exemplo, analisar apenas uma pasta que contenha poucos ficheiros.
Análise de rootkit	Localizações importantes do sistema onde um item suspeito possa representar um problema de segurança. Analisa ficheiros, pastas, unidades ou processos ocultos	Quando suspeita que um rootkit pode estar instalado no seu computador. Por exemplo, se tiver sido detectado malware recentemente no seu computador e quiser ter a certeza de que não foi instalado um rootkit.

Analisar no Explorador do Windows

Pode verificar se existem *vírus*, programas de *spyware* e *Riskware* em discos, pastas e ficheiros a partir do Windows Explorer.

Para verificar um disco, pasta ou ficheiro:

1. Coloque o ponteiro do rato e clique com o botão direito do rato no disco, pasta ou ficheiro que deseja verificar.
2. No menu de contexto, seleccione **Analisar pastas para detectar vírus**. (O nome da opção dependerá do que estiver a verificar; disco, pasta ou ficheiro.)
   Aparece a janela do **Assistente de Verificação** e a verificação pode começar.

Se for encontrado um *vírus* ou algum programa de *spyware*, o **Assistente de Verificação** orienta-o no processo de limpeza.

Seleccionar ficheiros a analisar

Pode seleccionar os tipos de ficheiro nos quais deve ser analisada a existência de *vírus* e *spyware* em análises manuais ou programadas.

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Outras definições** > **Análise manual**.
3. Em **Opções de análise**, opte entre as seguintes opções:

Analisar apenas tipos de ficheiros conhecidos	Para analisar apenas os ficheiros com maiores probabilidades de conterem infecções, por exempo, ficheiros executáveis. Ao seleccionar esta opção a análise torna-se mais rápida. São analisados os ficheiros com as seguintes extensões: `.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`.
Analisar no interior de ficheiros comprimidos	Para analisar ficheiros e pastas de arquivo.

Utilizar heurísticas avançadas	Para utilizar todas as heurísticas disponíveis durante a análise para encontrar mais facilmente malware recente ou desconhecido. **Nota:** Se seleccionar esta opção, a análise demora mais tempo e pode resultar num número mais elevado de falsos positivos (ficheiros inofensivos reportados como suspeitos).

4. Clique em **OK**.

Nota: Os ficheiros excluídos na lista de itens excluídos não são analisados mesmo que seleccione que sejam analisados aqui.

O que fazer quando são encontrados ficheiros nocivos

Seleccione como pretende tratar os ficheiros nocivos quando forem detectados.

Para seleccionar a acção a tomar quando são detectados conteúdos nocivos durante a análise manual:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Outras definições** > **Análise manual**.
3. Em **Quando vírus ou spyware é detectado**, seleccione entre as seguintes opções:

Opção	Descrição
Perguntar-me (predefinição)	Pode seleccionar a acção a ser tomada para cada item que é detectado durante a análise manual.
Limpar os ficheiros	O produto tenta desinfectar automaticamente os ficheiros infectados que são detectados durante a análise manual. **Nota:** Se o produto não conseguir limpar o ficheiro infectado, é colocado em quarentena (excepto quando detectado em unidades de rede ou amovíveis), para que não possa danificar o computador.
Colocar os ficheiros em quarentena	O produto move quaisquer ficheiros nocivos que são detectados durante a análise manual para a quarentena, onde não podem danificar o computador.
Eliminar automaticamente	O produto elimina quaisquer ficheiros nocivos que são detectados durante a análise manual.
Só relatório	O produto deixa quaisquer ficheiros nocivos que são detectados durante a análise manual como estão e regista a detecção no relatório da análise. **Nota:** Se a análise em tempo real estiver desactivada, qualquer malware pode danificar o computador se seleccionar esta opção.

Nota: Quando são detectados ficheiros nocivos durante a análise programada, são limpos automaticamente.

Programar uma análise

Configure o computador para analisar e remover vírus e outras aplicações nocivas automaticamente quando não os utilizar ou configure a análise para ser executada periodicamente para garantir que o computador esteja limpo.

Para programar uma análise:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Outras definições** > **Análise programada**.
3. Activar a **Análise programada**.
4. Seleccione quando pretende que a análise seja iniciada.

Opção	Descrição
Diariamente	Analisar o computador todos os dias.
Semanalmente	Analisar o computador nos dias da semana seleccionados. Seleccione os dias na lista.
Mensalmente	Analisar o computador nos dias do mês seleccionados. Para seleccionar os dias: 1. Selecção uma das opções em **Dia**. 2. Seleccione o dia do mês na lista ao lado do dia seleccionado.

5. Seleccione quando pretende iniciar a análise nos dias seleccionados.

Opção	Descrição
Hora de início	Iniciar a análise na hora especificada.
Quando um computador não é utilizado para	Iniciar a análise depois de não ter utilizado o computador durante o período de tempo especificado.

A análise programada utiliza as definições da análise manual quando analisa o computador, excepto se analisar sempre os ficheiros e limpar os ficheiros nocivos automaticamente.

Analisar mensagens de correio electrónico

A análise de mensagens de correio electrónico protege-o contra a recepção de ficheiros nocivos em mensagens de correio electrónico que lhe são enviadas.

A análise de vírus e spyware deve ser activada para analisar as mensagens de correio electrónico para detectar a existência de vírus.

Para activar a análise de correio electrónico:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Seleccione **Remover anexos nocivos de mensagens de correio electrónico**.
4. Clique em **OK**.

Quando são as mensagens de correio electrónico e os anexos analisados?

A análise de vírus e spyware pode remover conteúdos nocivos de mensagens de correio electrónico que receba.

A análise de vírus e spyware remove mensagens de correio electrónico nocivas que são recebidas por programas de correio electrónico como o Microsoft Outlook e Outlook Express, Microsoft Mail ou Mozilla Thunderbird. Analisa mensagens de correio electrónico encriptadas e anexos sempre que o programa de correio electrónico as recebe a partir do servir de correio utilizando o protocolo POP3.

A análise de vírus e spyware não pode analisar mensagens de correio electrónico no webmail, que incluem aplicações de correio electrónico que são executadas no navegador da Internet, como Hotmail, Yahoo! mail ou Gmail. Continua protegido contra *vírus* mesmo que não remova anexos nocivos ou que esteja a utilizar o webmail. Quando abre anexos de correio electrónico, a análise em tempo real remove quaisquer anexos nocivos antes de poderem causar qualquer dano.

Nota: A análise em tempo real protege apenas o computador mas não protege os seus amigos. A análise em tempo real não analisa os ficheiros anexos a menos que abra o anexo. Isto significa que se estiver a utilizar o webmail e reencaminhar uma mensagem antes de abrir o respectivo anexo, pode estar a reencaminhar uma mensagem de correio electrónico infectada para os seus amigos.

Visualizar os resultados da análise

O histórico de vírus e spyware apresenta todos os ficheiros nocivos que o produto tenha detectado.

Por vezes, o produto não pode efectuar a acção que tenha seleccionado quando algo nocivo é detectado. Por exemplo, se seleccionar limpar os ficheiros e não for possível limpar um ficheiro, o produto move-o para a quarentena. Pode visualizar estas informações no histórico de vírus e spyware.

Para ver o histórico:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Clique em **Visualizar histórico de remoção**.

O histórico de vírus e spyware apresenta as seguintes informações:

- data e hora em que foi detectado o ficheiro nocivo,
- o nome do malware e a respectiva localização no computador e
- a acção efectuada.

Como excluir ficheiros da análise

Por vezes pode pretender excluir alguns ficheiros ou aplicações da análise. Os itens excluídos não são analisados a menos que os remova da lista de itens excluídos.

Nota: As listas de exclusão são independentes da análise manual e da análise em tempo real. Por exemplo, se excluir um ficheiro da análise em tempo real, o ficheiro é analisado durante a análise manual, a menos que também o exclua da análise manual.

Excluir tipos de ficheiro

Quando exclui ficheiros pelo respectivo tipo, os ficheiros com as extensões especificadas não são analisados para detectar conteúdos nocivos.

Para adicionar ou remover um tipo de ficheiro que pretenda excluir:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione se pretende excluir o tipo de ficheiro da análise em tempo real ou manual:

   - Seleccione **Segurança do computador** > **Análise de vírus e spyware** para excluir o tipo de ficheiro da análise em tempo real.

- Seleccione **Outras definições** > **Análise manual** para excluir o tipo de ficheiro da análise manual.

3. Clique em **Excluir ficheiros da análise**.
4. Para excluir um tipo de ficheiro:
   a) Seleccione o separador **Tipos de Ficheiro**.
   b) Seleccione **Excluir ficheiros com estas extensões**.
   c) Introduza uma extensão de ficheiro que identifique o tipo de ficheiro que deseja excluir, no campo junto ao botão **Adicionar**.

      Para especificar ficheiros que não possuem extensão, introduza '.'. Pode utilizar o caracter '?' para representar qualquer caracter único ou '*' para representar qualquer número de caracteres.

      Por exemplo, para excluir ficheiros executáveis, introduza `exe` no campo.
   d) Clique em **Adicionar**.
5. Repita o passo anterior para qualquer outra extensão que deseje excluir da análise de vírus.
6. Clique em **OK** para fechar a caixa de diálogo **Excluir da Verificação**.
7. Clique em **OK** para aplicar as novas definições.

Os tipos de ficheiros seleccionados são excluídos de próximas análises.

Excluir ficheiros por localização

Quando exclui ficheiros pela localização, os ficheiros na unidade ou pastas especificadas não são analisados para detectar a existência de conteúdos nocivos.

Para adicionar ou remover localizações de ficheiros que pretende excluir:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione se pretende excluir a localização da análise em tempo real ou manual:
   - Seleccione **Computador** > **Análise de vírus e spyware** para excluir a localização da análise em tempo real.
   - Seleccione **Computador** > **Análise manual** para excluir a localização da análise manual.
3. Clique em **Excluir ficheiros da análise**.
4. Para excluir um ficheiro, unidade ou pasta:
   a) Seleccione o separador **Objectos**.
   b) Seleccione **Excluir objectos (ficheiros, pastas, ...)**.
   c) Clique em **Adicionar**.
   d) Seleccione o ficheiro, unidade ou pasta que pretende excluir da análise de vírus.

      Nota: Algumas unidades podem ser unidades amovíveis, como unidades de CD, DVD ou rede. As unidades de rede e as unidades amovíveis vazias não podem ser excluídas.

   e) Clique em **OK**.
5. Repita o passo anterior para excluir outros ficheiros, unidades ou pastas de serem analisados para detectar vírus.
6. Clique em **OK** para fechar a caixa de diálogo **Excluir da Verificação**.
7. Clique em **OK** para aplicar as novas definições.

Os ficheiros, unidades ou pastas seleccionados são excluídos de análises futuras.

Ver aplicações excluídas

Pode visualizar aplicações que tenha excluído da análise e removê-las da lista de itens excluídos se pretender analisá-los posteriormente.

Se a análise em tempo real ou manual detectar uma aplicação que se comporte como spyware ou riskware mas que saiba ser segura, pode excluí-la da análise para que o produto não o avise novamente acerca da aplicação.

Nota: Se a aplicação se comportar como um vírus ou outro software malicioso, não pode ser excluída.

Não pode excluir aplicações directamente. As novas aplicações são apresentadas na lista de exclusão apenas se as excluir durante a análise.

Para ver as aplicações excluídas da análise:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione se pretende visualizar as aplicações que foram excluídas da análise em tempo real ou manual:
   - Seleccione **Computador** > **Análise de vírus e spyware** para visualizar aplicações que tenham sido excluídas da análise em tempo real.
   - Seleccione **Computador** > **Análise manual** para visualizar aplicações que tenham sido excluídas da análise manual.
3. Clique em **Excluir ficheiros da análise**.
4. Seleccione o separador **Programas**.

   Nota: Só as aplicações de spyware e riskware é que podem ser excluídas, e não o vírus.

5. Se pretender analisar a aplicação excluída novamente:
   a) Seleccione a aplicação que pretende incluir na análise.
   b) Clique em **Remover**.
6. Clique em **OK** para fechar a caixa de diáologo **Excluir da Verificação**.
7. Clique em **OK** para sair.

Como utilizar a quarentena

A Quarentena é um repositório seguro para ficheiros potencialmente perigosos.

Os ficheiros em Quarentena não podem espalhar-se nem causar danos no computador.

Pode colocar *Malware*, *spyware* e *Riskware* em quarentena, tornando-os inofensivos. E mais tarde restaurar aplicações ou ficheiros da quarentena, se necessitar deles.

Quando um item em Quarentena não é necessário, pode eliminá-lo. Eliminar um item da Quarentena, remove-o irreversivelmente do computador.

- Normalmente, o itens de *Malware* em Quarentena podem ser eliminados.
- Na maioria dos casos, poderá eliminar programas de *spyware* em Quarentena. No entanto, pode acontecer que alguns programas de *spyware* tenham ocupado partes de software legítimo e, eliminá-los cessaria o funcionamento desse software. Para manter o software em funcionamento, esses programas de *spyware* podem ser retirados de Quarentena.

- O *Riskware* em quarentena também pode ser um programa legítimo. Se tiver instalado e configurado o programa, pode retirá-lo de Quarentena. Se o *Riskware* tiver sido instalado sem o seu conhecimento, o mais provável é que tenha sido instalado com más intenções e deve eliminá-lo.

Ver itens em quarentena

Pode ver mais informações sobre itens em Quarentena.

Para ver informações detalhadas sobre itens em Quarentena:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Clique em **Visualizar quarentena**.
   A página **Quarentena** apresenta o número total de itens guardados na quarentena.
4. Para visualizar informações detalhadas acerca dos items em quarentena, clique em **Detalhes**.

   Pode ordenar os conteúdos pelo nome do malware ou pelo caminho do ficheiro.

   É apresentada uma lista dos primeiros 500 itens com o tipo de itens em quarentena, o nome e o caminho no qual estão instalados os ficheiros.
5. Para visualizar mais informações acerca de um item em quarentena, clique no ícone próximo do item na coluna **Estado**.

Restaurar itens em quarentena

Pode restaurar itens em Quarentena, se for necessário.

Pode restaurar aplicações ou ficheiros em Quarentena se necessitar deles. Não restaure itens em Quarentena se não tiver a certeza de que não representam qualquer perigo. Os itens restaurados são movidos para a sua localização original.

Restaurar itens em quarentena:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **Análise de vírus e spyware**.
3. Clique em **Visualizar quarentena**.
4. Seleccione os itens em quarentena que deseja restaurar.
5. Clique em **Restaurar**.

O que é o DeepGuard

A aplicação DeepGuard analisa os conteúdos de ficheiros e o comportamento de aplicações e monitoriza aplicações que não são de confiança.

A aplicação DeepGuard bloqueia *vírus*, *worms* e outras aplicações nocivas novas e não descobertas que tentam efectuar alterações ao computador e impede que aplicações suspeitas acedam à Internet.

Quando a aplicação DeepGuard detecta uma nova aplicação que tenta potencialmente efectuar alterações nocivas ao sistema, permite que a aplicação seja executada numa zona segura. Na zona segura, a aplicação não pode danificar o computador. A aplicação DeepGuard analisa quais as alterações que foram tentadas

e, com base nas mesmas, decide quais as probabilidades da aplicação conter *malware*. Se a aplicação tiver probabilidades de conter *malware*, a aplicação DeepGuard bloquei-a.

As alterações potencialmente nocivas para o sistema que a aplicação DeepGuard detecta incluem:

- alterações de definições do sistema (registo do Windows),
- tenta desligar programas importantes do sistema como, por exemplo, programas de segurança como este produto, e
- tenta editar ficheiros importantes do sistema.

Activar ou desactivar a aplicação DeepGuard

Mantenha a aplicação DeepGuard activa para impedir que aplicações suspeitas procedam a alterações potencialmente nocivas no sistema do computador.

Se tiver o Windows XP, certifique-se de ter o Service Pack 2 instalado antes de activar a aplicação DeepGuard.

Para activar ou desactivar a aplicação DeepGuard:

1. Na página principal, clique em **Estado**.
2. Clique em **Alterar definições nesta página**.

   Nota: Precisa de ter direitos de administrador para desactivar as funcionalidades de segurança.

3. Activar ou desactivar a aplicação **DeepGuard**.
4. Clique em **Fechar**.

Permitir aplicações que a aplicação DeepGuard tenha bloqueado

Pode controlar quais as aplicações que a aplicação DeepGuard permite ou bloqueia.

Por vezes a aplicação DeepGuard pode bloquear uma aplicação segura e impedir que seja executada, mesmo que pretenda utilizar a aplicação e saiba que é segura. Isto acontece porque a aplicação tenta proceder a alterações no sistema que podem ser potencialmente nocivas. Também pode ter bloqueado não intencionalmente a aplicação quando tenha sido apresentada uma mensagem pendente da aplicação DeepGuard.

Para permitir a aplicação que a aplicação DeepGuard tenha bloqueado:

1. Na página principal, clique em **Ferramentas**.
2. Clique em **Aplicações**.
   É apresentada a lista **Programas monitorizados**.
3. Localize a aplicação que pretende permitir.

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

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

A aplicação DeepGuard permite que a aplicação proceda a alterações no sistema novamente.

Utilize a aplicação DeepGuard no modo de compatibilidade

Para uma máxima protecção, a aplicação DeepGuard modifica temporariamente os programas em execução. Alguns programas verificam se não são corrompidos ou modificados e podem não ser compatíveis com esta funcionalidade. Por exemplo, os jogos online com ferramentas anti-fraude verificam se não foram modificados de alguma forma quando são executados. Nestes casos, pode activar o modo de compatibilidade.

Para activar o modo de compatibilidade:

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

   Nota: Precisa de direitos de administrador para alterar as definições.

2. Seleccione **Segurança do computador** > **DeepGuard**.
3. Seleccione **Utilizar o modo de compatibilidade**.
4. Clique em **OK**.

O que fazer com avisos de comportamentos suspeitos

A aplicação DeepGuard monitoriza aplicações que não são de confiança. Se uma aplicação monitorizada tentar aceder à Internet, tentar efectuar alterações ao sistema ou se comportar de forma suspeita, a aplicação DeepGuard bloqueia a aplicação.

Quando tiver seleccionado **Avisar-me acerca de comportamentos suspeitos** nas definições da aplicação DeepGuard, a aplicação DeepGuard notifica-o quando detectar uma aplicação potencialmente nociva ou quando inicia uma aplicação que tenha uma reputação desconhecida.

Para decidir o que fazer com a aplicação que a aplicação DeepGuard tenha bloqueado:

1. Clique em **Detalhes** para visualizar mais informações acerca do programa.
   A secção de detalhes apresenta:
   - a localização da aplicação,
   - a reputação da aplicação na Rede de protecção em tempo real e
   - quão comum é a aplicação.
2. Decida se confia na aplicação que a aplicação DeepGuard tenha bloqueado:
   - Seleccione **Confio na aplicação. Permitir que continue.** se não pretender bloquear a aplicação.

     É mais provável que a aplicação seja segura se:

     - A aplicação DeepGuard bloqueou a aplicação como resultado de algo que tenha feito,
     - reconhece a aplicação ou
     - obteve a aplicação a partir de uma fonte de confiança.
   - Seleccione **Não confio na aplicação. Manter a aplicação bloqueada.** se pretender manter a aplicação bloqueada.

     É mais provável que a aplicação não seja segura se:

     - a aplicação não for comum,
     - a aplicação tiver uma reputação desconhecida ou
     - não conhecer a aplicação.
3. Se pretender enviar uma aplicação suspeita para análise:
   a) Clique em **Reportar a aplicação à F-Secure**.
   O produto apresenta as condições de envio.
   b) Clique em **Aceito** se concordar com as condições e pretender enviar a amostra.

   Recomendamos que envie uma amostra quando:

   - A aplicação DeepGuard bloquear uma aplicação que saiba ser segura ou
   - suspeitar que a aplicação possa ser *malware*.