GUIA DO USUÁRIO

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

Guia do Usuário

Publication date 04/29/2024

Aviso Legal

Bitdefender

Índice

SOBRE ESTE GUIA

Propósito e público-alvo

Este guia destina-se a todos os usuários da Bitdefender que escolheram o Controle dos Pais do Bitdefender como sua solução para a segurança, monitoramento e proteção contínua dos dispositivos e da presença on-line de seus filhos.

Você descobrirá como instalar, configurar e aproveitar ao máximo o Controle dos Pais do Bitdefender, para obter recursos aprimorados e um melhor controle sobre as atividades on-line de seus filhos.

Desejamos-lhe uma agradável e útil leitura.

Como usar este guia

Este guia é organizado em diversos tópicos importantes:

Introdução (página 4)

Comece a configurar o Controle dos Pais do Bitdefender.

Recursos e Funcionalidades (página 10)

Saiba como usar o Controle dos Pais do Bitdefender e todos os seus recursos.

Conseguindo ajuda (página 22)

Onde procurar e onde pedir ajuda caso algo aconteça fora do esperado.

Convenções utilizadas neste guia

Convenções Tipográficas

São utilizados diversos estilos de texto neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.

Aparência	Descrição
sample syntax	As amostras de sintaxe são impressas com monospaced personagens.
https://www.bitdefender.com	A hiperligação URL aponta para uma localização externa em servidores http ou ftp.
documentation@bitdefender.com	Endereços de email são inseridos no texto para contactar a solicitar mais informação.
Sobre este Guia (página 1)	Esta é uma hiperligação interna que o leva para uma localização dentro do documento.
filename	Arquivos e diretórios são impressos usando monospaced Fonte.
opção	Todas as opções de produtos são impressas usando **audacioso** personagens.
palavra-chave	Palavras-chave ou frases importantes são destacadas usando **audacioso** personagens.

Avisos

Os avisos estão em notas internas do texto, com marcação gráfica, que chamam a sua atenção para informações adicionais relacionadas ao parágrafo atual.

Observação

A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

Importante

Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, providencia-lhe informação bastante importante.

Aviso

Trata-se de informação critica que deve de tratar com cuidados redobrados. Nada de negativo acontecerá se você seguir as indicações. Deve de lê-lo e compreendê-lo, porque descreve algo extremamente arriscado.

Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificamos e testamos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a si a melhor documentação possível.

Informe-nos enviando um e-mail para documentation@bitdefender.com. Escreva todos os seus e-mails relacionados à documentação em inglês para que possamos processá-los com eficiência.

1. INTRODUÇÃO

Começaremos com um guia detalhado e passo a passo sobre como configurar a assinatura do Controle dos Pais do Bitdefender na sua conta central do Bitdefender. Essa é a primeira etapa do processo simples que é necessário para garantir que você possa gerenciar e monitorar as atividades on-line de seus filhos de forma eficaz.

1.1. Configuração do Controle dos Pais

Ao ativar sua assinatura, para começar a configurar o Controle dos Pais do Bitdefender em sua conta:

1. Vá para a sua conta da Bitdefender Central e acesse a guia **Controle dos Pais** no lado esquerdo da tela.
2. Clique em **Começar**.
3. Defina um PIN do aplicativo.

   > **Atenção**
   > Esse código PIN ajudará a evitar que seus filhos desativem os recursos de controle dos pais por conta própria, fazendo logout do aplicativo infantil.
   >
   > Memorize esse PIN.

4. Clique em **Próximo**.
5. Prossiga criando um perfil infantil. Digite o nome da criança e selecione uma foto de perfil. Em seguida, clique em **Próximo**.
6. Selecione a idade que corresponde à da criança. Quando terminar, clique em **Próximo**.
7. Indique se o aplicativo Controle dos Pais deve ser instalado no dispositivo atual que você está usando ou em outro dispositivo.

Atenção

Se você selecionar **Outros dispositivos**, serão apresentadas três opções de instalação. Selecione o método preferido:

- Lendo o QR code.
- Copiando o link fornecido e abrindo-o no navegador do dispositivo da criança.
- Enviando o link de instalação por e-mail.

8. Aguarde a conclusão do download e, em seguida, execute o instalador no dispositivo em questão.

A partir daí, o processo de instalação será iniciado. As etapas que precisam ser executadas a partir daqui variam de acordo com o tipo de dispositivo e o sistema operacional no qual a instalação está sendo realizada.

1.2. Instalação do Controle dos Pais do Bitdefender nos dispositivos de seus filhos

1.2.1. Em dispositivos Windows:

Depois de executar o instalador recém-baixado:

1. Clique em **Sim** se uma caixa de diálogo de controle de conta de usuário solicitar que você permita que o arquivo de instalação faça alterações no dispositivo.
2. Faça login com as credenciais de sua conta da Bitdefender Central, se solicitado.

1.2.2. Em dispositivos macOS:

Quando o download do instalador for concluído, clique duas vezes no arquivo do Bitdefender para iniciar o processo de instalação:

1. Você será guiado pelas etapas necessárias para instalar o Controle dos Pais do Bitdefender para macOS. Clique em **Permitir** se for solicitado.
2. Clique nos dois botões **Continuar** consecutivos.

3. Para continuar a instalação, você terá que concordar com os termos do acordo de assinatura do software.
4. Clique em **Continuar**. Depois disso, clique em **Instalar**.
5. Quando solicitado, digite um nome de administrador e uma senha e pressione o botão **Instalar Software**.

Aguarde até receber uma notificação pop-up de que *uma extensão do sistema foi bloqueada*. Essa é uma ocorrência natural durante esse procedimento. Para continuar, você deve permitir a extensão do sistema de Controle dos Pais conforme as instruções abaixo:

1. Clique no botão **Abrir Configurações do Sistema**.

> **Atenção**
> Nas versões anteriores do macOS, esse botão é chamado de **Abrir Preferências de Segurança**.

2. Clique no botão **Permitir** janelas exibidas na tela e, em seguida, insira um nome de administrador e uma senha para desbloquear as configurações.

> **Atenção**
> No macOS 11 (Big Sur) e no macOS 12 (Monterey), antes de clicar no botão **Permitir**, você precisa clicar no ícone de cadeado no canto inferior esquerdo da janela **Segurança e Privacidade** e, em seguida, inserir um nome de administrador e uma senha para fazer alterações.

3. A janela pop-up **Filtrar conteúdo de rede** será exibida. Clique no botão **Permitir** nessa janela.
4. Em seguida, clique no botão **Abrir configurações do sistema**.
5. Clique no botão **Permitir** mais uma vez.

1.2.3. Em dispositivos Android:

Você encontrará a página da Google Play Store do Bitdefender para o aplicativo Controle dos Pais:

1. Toque no botão **Instalar**. O aplicativo começará a ser baixado e instalado.

2. Quando a instalação for concluída, você verá um botão **Abrir**. Toque nele para iniciar o aplicativo Controle dos Pais do Bitdefender.

Depois de abrir o aplicativo, siga as etapas na tela para configurar o Controle dos Pais no dispositivo Android do seu filho:

1. Toque em **Continuar**.
2. Entre no aplicativo usando as credenciais de sua conta da Bitdefender Central.
3. Selecione o perfil infantil que você deseja atribuir ao dispositivo Android.
4. Você precisará conceder as permissões necessárias ao aplicativo para que ele funcione corretamente. Para fazer isso, toque em **Próximo** e depois em:
    a. Permita acesso à VPN e, em seguida, escolha **Permitir sempre** para filtrar o conteúdo on-line no dispositivo de seu filho.
    b. Para ajudar a localizar o dispositivo Android de seu filho, toque em **Próximo**, depois em **Permitir** e escolha a opção **Permitir sempre**.
    c. As permissões de VPN e Localização exibirão uma marca de seleção verde. Toque em **Concluir configuração** e, em seguida, toque em **Próximo**.
    d. Nesse ponto, há mais 3 permissões para bloquear o acesso à internet e aos aplicativos no dispositivo da criança. Toque em **Definir permissão** no painel **Direitos do administrador do dispositivo**.
    e. Toque no botão **Concluir** quando terminar de configurar o aplicativo Controle dos Pais do Bitdefender.

1.2.4. Em dispositivos iOS:

Você encontrará a página da App Store do Bitdefender para o aplicativo Controle dos Pais:

1. Toque no ícone de nuvem com uma seta apontando para baixo. O aplicativo começará a ser baixado e instalado.
2. Quando a instalação for concluída, você verá um botão **Abrir**. Toque nele para iniciar o aplicativo Controle dos Pais do Bitdefender.

3. Se algum perfil do Gerenciamento de Dispositivo Móvel for encontrado no dispositivo iOS da criança, você será solicitado a removê-lo. Toque em **Próximo** e escolha **Remover perfis**.
4. No aplicativo de **Configurações** do iOS, vá para **Geral**, role para baixo e toque na seção **VPN e Gerenciamento de Dispositivos**.
5. Toque em cada entrada na seção **GERENCIAMENTO DE DISPOSITIVO MÓVEL** e escolha **Remover gerenciamento** para cada uma delas.
   Repita esse processo até que não haja mais entradas no GERENCIMENTO DE DISPOSITIVO MÓVEL.

Reabra o aplicativo instalado no dispositivo da criança e siga as etapas na tela para configurar o Controle dos Pais do Bitdefender:

1. Toque em **Continuar**.
2. Faça login no aplicativo usando as credenciais da sua conta da Bitdefender Central.
3. Selecione o perfil infantil que você deseja atribuir ao dispositivo iOS.
4. Em seguida, você precisará conceder as permissões necessárias para que o aplicativo funcione corretamente. Toque em **Próximo**.
5. Permita o acesso à VPN para filtrar o conteúdo on-line no dispositivo de seu filho. Toque em **Permitir** duas vezes seguidas para adicionar as configurações de VPN.
6. Toque em **Próximo** e escolha **Permitir** para ajudar a localizar o dispositivo iOS de seu filho.
7. Em seguida, passe pelo processo de configuração do Apple Family Control para bloquear o acesso à internet e aos aplicativos no dispositivo da criança.

   > **Atenção**
   > Você pode tocar em **Saiba como** para obter um guia passo a passo sobre como fazer isso.

8. Após configurar o Apple Family Control no seu próprio dispositivo e no dispositivo de seu filho, selecione **Já configurei o Apple Family Control** para continuar.

9. Em seguida, permita que o Acesso ao Tempo de Tela filtre o conteúdo on-line no dispositivo iOS de seu filho.

10 Toque em **Concluir configuração**.

.

Após concluir essas etapas no(s) dispositivo(s) de seu filho, o processo de configuração estará concluído. Como pai ou mãe, agora você pode monitorar as atividades on-line do seu filho e visualizar as estatísticas de uso na sua conta da Bitdefender Central, dentro do painel de Controle dos Pais, que será detalhado nos próximos capítulos.

2. RECURSOS E FUNCIONALIDADES

2.1. Perfis

Um perfil infantil é um conjunto personalizado de regras que permite que o aplicativo Controle dos Pais do Bitdefender gerencie e monitore as atividades on-line de uma criança. Ele inclui configurações adaptadas à idade da criança, como filtros de conteúdo e restrições de tempo. Usando a conta da Bitdefender Central, os pais podem criar, editar e excluir esses perfis, bem como atribuir e remover dispositivos a eles, garantindo uma experiência on-line segura e apropriada para seus filhos.

Para criar um perfil infantil:

1. Acesse a Bitdefender Central e faça login em sua conta.
2. No menu do lado esquerdo, clique na guia **Controle dos pais**.
3. Clique em **Novo perfil** para criar um novo perfil infantil.
4. Insira o nome da criança, a foto do perfil e a data de nascimento.

> **Atenção**
> Com base na idade da criança, o Bitdefender bloqueia automaticamente determinadas categorias, como bate-papo, redes sociais, conteúdo explícito e muito mais. Você pode ajustar as categorias bloqueadas posteriormente.

5. Clique no botão **Salvar**.

O novo perfil foi criado e aparecerá na página.

Para editar um perfil infantil:

1. Clique no botão **Exibir detalhes** no perfil da criança.
2. Para modificar o perfil de seu filho, vá para **Editar perfil**.
3. Use o campo correspondente para alterar o nome, a data de aniversário e/ou a foto do perfil da criança.
4. Clique em **Salvar alterações** depois de alterar os detalhes necessários.

Para excluir um perfil infantil:

1. Clique no botão **Exibir detalhes** no perfil da criança.
2. Vá para **Editar perfil**.
3. Clique no botão **Excluir perfil** e confirme a exclusão.

Para atribuir dispositivos a um perfil infantil:

Se seu filho tiver vários dispositivos (Windows, macOS, Android ou iOS), você poderá atribuí-los ao mesmo perfil infantil.

1. Clique no botão **Exibir detalhes** no perfil da criança.
2. Clique no número de dispositivos listados sob seus nomes.
3. Clique no botão **Atribuir dispositivos**.
4. Selecione o nome do dispositivo e clique no botão **Atribuir**.

> **Atenção**
> Se o dispositivo não estiver visível na lista, clique em **Instalar um novo dispositivo** e siga as instruções na tela para instalar e configurar o Controle dos Pais do Bitdefender no novo dispositivo.

Para remover dispositivos de um perfil infantil:

Quando você remove um dispositivo do perfil de uma criança, isso significa que o dispositivo não estará mais sob o gerenciamento do Controle dos Pais do Bitdefender. As regras e configurações especificadas no perfil da criança não se aplicarão mais a esse dispositivo. Embora o aplicativo Controle dos Pais permaneça instalado no dispositivo, ele deixa de funcionar.

1. Clique no botão **Exibir detalhes** no perfil da criança.
2. Clique no número de dispositivos listados sob seus nomes.
3. Localize o dispositivo da criança e clique na opção **Desatribuir dispositivo**.
4. Pressione o botão **Sim, desatribuir dispositivo** para confirmar a ação.

2.2. Estatísticas

O Controle dos Pais fornece informações sobre como as crianças utilizam a internet e seus dispositivos. Neste guia, vamos nos aprofundar nas várias estatísticas disponíveis para os pais na Bitdefender Central, capacitando-os a tomar decisões bem informadas e a garantir uma experiência on-line segura e equilibrada para seus filhos.

Para visualizar as estatísticas:

1. Acesse a Bitdefender Central e faça login em sua conta.
2. Depois de fazer login, clique na guia **Controle dos pais** no menu do lado esquerdo.
3. Clique no perfil da criança cujas estatísticas você deseja visualizar.

Ao selecionar o perfil do seu filho, você será direcionado a um painel que exibe vários painéis de estatísticas. Todos se referem aos outros recursos descritos mais adiante nesta documentação.

2.3. Código PIN dos pais

O código PIN dos pais é um recurso de segurança dentro do painel de Controle dos Pais da plataforma Bitdefender Central. Ele serve como um meio para que os pais mantenham o controle sobre o acesso de seus filhos ao aplicativo Controle dos Pais do Bitdefender instalado em seus dispositivos. Veja abaixo um guia detalhado sobre como definir, localizar e gerenciar o PIN dos pais.

O código PIN dos pais evita logouts não autorizados do aplicativo Controle dos Pais do Bitdefender no dispositivo de seu filho. Quando seu filho tentar fazer logout, ele será solicitado a digitar esse código PIN. Isso garante que somente você, como pai ou mãe com acesso à conta da Bitdefender Central, possa controlar as configurações do aplicativo.

> **Atenção**
> Ao configurar o aplicativo Controle dos Pais pela primeira vez, você será solicitado a estabelecer um PIN Parental de 4 a 8 dígitos.

2.3.1. Esqueceu o código PIN?

Caso esqueça o código PIN, você pode recuperá-lo facilmente na sua conta da Bitdefender Central:

1. Acesse a Bitdefender Central e faça login em sua conta.
2. Uma vez conectado, clique na guia **Controle dos pais** no menu do lado esquerdo.
3. No canto superior direito da página, clique em **Código PIN**.
4. Clique no ícone em forma de olho para encontrar o código PIN dos pais.

2.3.2. Alterando seu código PIN

Se você suspeitar que seu código PIN foi comprometido ou simplesmente quiser atualizá-lo por motivos de segurança:

1. Na seção Controle dos Pais da sua conta Bitdefender Central, clique na opção **Código PIN**.
2. Escolha a opção **Alterar PIN** e siga as instruções na tela para definir um novo código PIN.

2.4. Filtro de Conteúdo

A filtragem de conteúdo permite que os pais restrinjam o acesso de seus filhos ao conteúdo on-line, de modo que eles possam bloquear categorias inteiras de sites ou fazer exceções com base em URLs ou tópicos específicos.

> **Atenção**
> O recurso de Filtragem de Conteúdo do Controle dos Pais do Bitdefender não impede que seu filho use aplicativos ou sites off-line, pois ele apenas gerencia o tráfego on-line da internet dos dispositivos que ele usa.

Para acessar o Filtro de Conteúdo:

1. Faça login em sua conta da Bitdefender Central.
2. No menu do lado esquerdo, clique na guia **Controle dos pais**.
3. Acesse o perfil da criança e clique no menu **Mais** no canto superior direito. Em seguida, selecione **Filtro de conteúdo**.

2.4.1. Pesquisa Segura e YouTube Restrito

Na seção **Privacidade e segurança**, no lado direito da tela, é possível ativar as opções Pesquisa Segura e YouTube Restrito.

- **Pesquisa segura:** ao usar mecanismos de pesquisa, a Pesquisa Segura impede a exibição de conteúdo considerado inseguro pelo Google nos resultados de pesquisa.
- **YouTube Restrito:** fornece à criança vídeos apropriados para a sua idade no YouTube.

> **Atenção**
> **A Pesquisa Segura** e o **YouTube Restrito** redirecionam todas as solicitações de DNS do **google.com** para **safe.google.com**. A filtragem real do conteúdo é feita pelo Google. O Controle dos Pais do Bitdefender não filtra o conteúdo da Pesquisa Segura ou do Google. Da mesma forma, o YouTube pode não controlar efetivamente as tags nos vídeos, expondo potencialmente as crianças a conteúdo inadequado.

2.4.2. Bloqueio e Permissão de Categorias de Sites

> **Atenção**
> Na seção **Categorias**, os tipos de site que seu filho pode ver on-line são permitidos ou bloqueados por padrão, dependendo da idade definida quando o perfil da criança foi criado.

Você pode bloquear ou permitir vários tipos de site a qualquer momento:

1. Selecione uma categoria.
2. Para bloquear o acesso a essa categoria, selecione **Bloqueado** no menu suspenso. Para permitir o acesso, selecione **Permitido**.

> **Importante**
> Se você bloquear a categoria **Compartilhamento de arquivos** do perfil do seu filho, a atualização do macOS não funcionará. Recomendamos permitir temporariamente o Compartilhamento de Arquivos ao atualizar o macOS.

2.4.3. Exceções

Na guia **Exceções**, é possível definir exclusões de sites e aplicativos:

- **Adicionar exceções de site:**
  1. Clique no botão **Adicionar exceção**.
  2. Selecione **Somente site** e clique no botão **Próximo**.
  3. Digite o endereço do site e selecione se deseja permitir ou bloqueá-lo no menu suspenso.
  4. Em seguida, clique no botão **Adicionar**.
- **Exceções de apps e plataformas web:**
  1. Clique no botão **Adicionar exceção**.

2. Selecione **Plataforma web e aplicativos** e clique no botão **Próximo**.
3. Escolha a plataforma para a qual você deseja abrir uma exceção na lista fornecida. Como alternativa, use a barra de pesquisa para encontrar o que você está procurando.
4. Em seguida, clique no botão **Adicionar**.

- **Remover exceções:**
  Todas as exceções que você configurar aparecerão no Filtro de Conteúdo dentro da lista designada na parte inferior.
  Para excluir uma exceção, basta clicar no ícone de lixeira localizado à direita da entrada.

2.5. Tempo diário de internet

Na sua conta da Bitdefender Central, na seção Controle dos pais, para cada perfil infantil criado, é exibido um cartão de Tempo diário de internet. Esse cartão mostra o tempo total que a criança passou on-line em todos os dispositivos atribuídos. Para limitar o tempo on-line de uma criança:

1. Vá até o perfil da criança e clique no botão **Definir limite de tempo** no painel **Tempo diário de internet**. Como alternativa, você pode clicar no menu **Mais** no canto superior direito e selecionar **Tempo diário de internet**.
2. Clique no botão **Ativar limite de tempo** para ativar esse recurso.

> **Atenção**
> Por padrão, a criança recebe 1 hora e 30 minutos de acesso à internet por dia. Se os pais não estenderem esse limite de tempo, o acesso da criança à internet será interrompido após atingir a marca de 1 hora e 30 minutos.

Remoção do limite de tempo diário:

- Para desativar o recurso de tempo diário de internet, acesse o painel do perfil de seu filho, clique no botão **Editar tempo** no painel **Tempo diário de internet** e, em seguida, pressione o botão **Pausar** no painel **Limite de tempo**.

- Para remover o limite de tempo de um determinado dia, clique no botão ⊗ correspondente a esse dia da semana no painel **Programação**.

Alteração do limite de tempo:

- Para definir um limite de tempo diferente para um dia específico da semana, clique no nome do dia no painel **Programação**, selecione o limite desejado no menu suspenso e clique no botão **Salvar alterações**. Você pode selecionar mais de um dia de cada vez.

2.5.1. Sistema de recompensas

O recurso **Recompensa** permite que você recompense ou estenda o tempo de tela do seu filho, promovendo hábitos on-line saudáveis. Você pode usar o sistema de recompensas de duas maneiras diferentes:

- **Recompensa manual:**

  1. Navegue até a seção Controle dos pais na sua conta da Bitdefender Central.
  2. Vá para o perfil da criança e clique no botão **Recompensa** no painel **Tempo diário de Internet**.
  3. Selecione a quantidade de tempo extra que deseja adicionar e confirme clicando em **Recompensa**.

- **Solicitação da criança:**
  Quando seu filho atingir o limite diário, ele poderá solicitar tempo adicional por meio do aplicativo Parental Control instalado no dispositivo móvel. Como pai ou mãe, você receberá uma notificação em sua conta da Bitdefender Central.

  1. Quando estiver conectado à sua conta da Bitdefender Central, procure um ponto vermelho no sino de notificações no canto superior direito da tela, indicando uma solicitação pendente de seu filho.
  2. Analise a solicitação e decida quanto tempo extra será concedido.

> **Atenção**
> As crianças têm a opção de solicitar extensões de seu tempo diário de internet somente em dispositivos Android e iOS.

2.6. Como desativar a internet no dispositivo de seu filho

Como pai ou mãe, gerenciar o uso da internet de seu filho pode ser importante para o bem-estar e a produtividade dele. Para desativar temporariamente o acesso à internet no dispositivo de seu filho usando o Controle dos Pais do Bitdefender:

1. Acesse a Bitdefender Central e faça login em sua conta.
2. Uma vez conectado, clique na guia **Controle dos pais** no menu do lado esquerdo.
3. Selecione **Exibir detalhes** no perfil da criança cuja internet você deseja desativar.
4. Clique no botão **Parar a Internet** no canto superior direito do painel da criança

   > **Atenção**
   > A internet será cortada em todos os dispositivos de seu filho. Essa ação substitui todas as configurações de Controle dos Pais existentes, como rotinas, limite de tempo diário ou categorias permitidas.

5. Quando o acesso à internet é cortado, o botão **Parar internet** é alterado para **Retomar internet**. Para restaurar o acesso à internet, basta clicar no botão **Retomar internet**.

2.7. Rotinas

No Controle dos Pais do Bitdefender, você pode definir até 3 rotinas distintas para programar quando o acesso à internet do seu filho será desativado. Elas oferecem uma abordagem estruturada para gerenciar as atividades on-line de uma criança, promovendo hábitos saudáveis e o envolvimento da família e, ao mesmo tempo, garantindo sua segurança. Essas rotinas são independentes umas das outras, o que significa que você pode optar por ativar apenas uma, duas ou todas as três, de acordo com suas preferências:

- **Tempo de foco**
  Crie um cronograma que inclua tempo para a lição de casa, estudo e outras atividades.

- **Hora de dormir**
  Use a rotina da hora de dormir para bloquear um período de descanso para seu filho.
- **Tempo em família**
  Use a rotina de tempo em família para reservar um tempo para que seu filho esteja presente durante as refeições em família, por exemplo.

> **Atenção**
> **Rotinas x tempo diário na internet:**
>
> Durante as rotinas, o tempo gasto on-line não é contabilizado no limite de tempo diário de Internet. Quando a rotina termina, a função Tempo diário de internet volta a contar o uso da internet pela criança.
>
> Para evitar confusão para os pais, enquanto uma rotina estiver em andamento, o cartão Tempo diário de internet não ficará visível no painel do perfil da criança até que a rotina seja concluída. Em vez disso, o nome da rotina ativa será exibido durante esse período.

2.7.1. Configurar rotinas

Para configurar qualquer uma das rotinas de controle dos pais:

1. Acesse a Bitdefender Central e faça login em sua conta.
2. No menu do lado esquerdo, clique na guia **Controle dos pais**.
3. Vá para o perfil da criança e selecione a rotina desejada no menu **Mais**.
4. Clique no botão **Ativar** para ativar a rotina selecionada.
5. Isso fará com que os painéis **Programação** e **Acesso à internet** sejam exibidos.
   - **Agendar:**
     Para definir uma rotina para um ou vários dias da semana:
     a. Selecione os dias desejados.
     b. Selecione os horários de início e término da rotina no menu suspenso fornecido.
     c. Por fim, clique no botão **Salvar alterações** para confirmar suas seleções.

     Para remover a rotina de um dia específico, clique no botão ⊗ correspondente a esse dia da semana.

- **Acesso à internet:**
  O painel de acesso à internet em uma rotina oferece duas funções principais para controlar as atividades on-line de uma criança durante períodos de tempo específicos:
  - **Desligamento completo da internet:** os pais têm a opção de desativar completamente o acesso à internet para seus filhos durante o horário de rotina programado. Ao desativar o **acesso à internet**, os dispositivos da criança não poderão acessar a internet dentro do período de tempo designado.
  - **Categoria ou site selecionados:** como alternativa, os pais podem optar por permitir o acesso à internet durante o horário de rotina, mas restringir determinados sites ou categorias de conteúdo. Quando você ativa o **acesso à internet**, duas guias adicionais, a saber, as guias **Categorias** e **Exceções**, ficam visíveis, dando acesso a outras configurações do Filtro de Conteúdo</link>. (página 13)

2.8. Rastreamento da localização de seu filho

Com a prevalência de smartphones e outros dispositivos móveis, o rastreamento da localização de seu filho tornou-se uma ferramenta essencial para muitas famílias. Seja para saber onde estão depois da escola ou durante as saídas com os amigos, ter a capacidade de monitorar a localização deles proporciona tranquilidade aos pais. Aqui está um guia passo a passo sobre como rastrear a localização de seu filho usando o recurso de localização do Controle dos Pais do Bitdefender.

1. Acesse a Bitdefender Central e faça login em sua conta.
2. Depois de fazer login, clique na guia **Controle dos pais** no menu do lado esquerdo.
3. Se você tiver vários filhos, selecione **Exibir detalhes** no perfil do filho cuja localização você deseja rastrear.
4. No painel Localização, selecione o dispositivo Android ou iOS que deseja rastrear e clique no botão **Localizar**.

> **Atenção**
> O recurso de localização do Controle dos Pais do Bitdefender não está disponível para dispositivos Windows e macOS.

5. Após uma breve espera, um pino vermelho indicará a localização atual de seu filho no mapa.

> **Atenção**
> As atualizações de localização ocorrem a cada 20 minutos. Se você tentar rastrear a localização do seu filho em menos de 20 minutos desde a localização anterior, a localização exibida poderá não refletir o paradeiro dele em tempo real.

3. DESINSTALAÇÃO DO CONTROLE DOS PAIS

Desinstalação do Controle dos Pais do Bitdefender em dispositivos Windows:

1. Remova o dispositivo do perfil de seu filho na Bitdefender Central.
2. Abra o Painel de Controle no dispositivo em questão e localize o Controle dos Pais do Bitdefender na lista **Programas e Recursos**.
3. Desinstale o Controle dos Pais do Bitdefender.

Desinstalação do Controle dos Pais do Bitdefender em dispositivos macOS:

1. Remova o dispositivo do perfil de seu filho na Bitdefender Central.
2. Abra o **Localizador** no dispositivo macOS.
3. Acesse seus Aplicativos e localize a pasta Bitdefender.
4. Abra-a e execute o **Desinstalador do Bitdefender**.
5. Escolha Controle dos Pais do Bitdefender na lista de produtos a serem desinstalados.
6. Forneça as credenciais de administrador e aguarde a conclusão da desinstalação.

Desinstalação do Controle dos Pais do Bitdefender em dispositivos Android e iOS:

1. Remova o dispositivo do perfil de seu filho na Bitdefender Central.
2. Desinstale o Controle dos Pais do dispositivo móvel como qualquer outro aplicativo ou por meio da Google Play Store ou da Appstore, respectivamente.

4. CONSEGUINDO AJUDA

4.1. Pedir Ajuda

O Bitdefender se empenha em oferecer aos seus clientes um nível incomparável de apoio preciso e rápido. Se tiver qualquer problema ou pergunta sobre o seu produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou uma resposta. Ao mesmo tempo, pode entrar em contacto com a equipe de Atendimento ao Cliente da Bitdefender. Os nossos representantes de apoio responderão às suas perguntas em tempo hábil e oferecerão a assistência de que precisa.

4.2. Recursos Em Linha

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte da Bitdefender:
  https://www.bitdefender.pt/consumer/support/
- A Comunidade de Especialistas da Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

4.2.1. Centro de Suporte da Bitdefender

A Bitdefender Support Center é um repositório de informação online acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das atividades de reparação de erros por parte da equipa técnica do suporte BitDefender e da equipa de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de ameaças, a administração de soluções BitDefender e explicações pormenorizadas e muitos outros artigos.

A Bitdefender Support Center encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma

outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na Bitdefender Support Center, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

O Centro de Suporte Bitdefender está disponível a qualquer momento no seguinte endereço: https://www.bitdefender.pt/consumer/support/.

4.2.2. A Comunidade de Especialistas da Bitdefender

A Comunidade de Especialistas da Bitdefender é um ambiente onde os utilizadores, entusiastas e fãs da Bitdefender podem interagir, trocar ideias, apoiar-se mutuamente e partilhar os seus conhecimentos e soluções. É também um lugar de criação de ideias que fornece um feedback valioso para as nossas equipas de desenvolvimento. Os membros da comunidade são utilizadores experientes da Bitdefender que têm todo o prazer em ajudar outros colegas no seu tempo livre. Com a sua imensa contribuição e os seus esforços genuínos e voluntários, criámos uma base de conhecimento onde os utilizadores podem encontrar respostas e orientação, mas com um toque humano.

Aqui encontrará conversas significativas com pessoas que utilizam a Bitdefender nos seus dispositivos. A comunidade oferece uma verdadeira ligação com os nossos membros e faz com que sua voz seja ouvida. É um lugar onde é encorajado a participar sabendo que sua opinião e sua contribuição são respeitadas e bem recebidas. Ao ser um fornecedor valioso, esforçamo-nos para oferecer um nível inigualável de apoio rápido e preciso e desejamos aproximar os nossos utilizadores de nós. Projetamos a nossa comunidade com este propósito em mente.

Pode encontrar a nossa página da Comunidade de Especialistas aqui:

https://community.bitdefender.com/en/

4.2.3. Bitdefender Cyberpedia

A Bitdefender Cyberpedia tem toda a informação de que precisa sobre as últimas ameaças cibernéticas. Este é o lugar onde os especialistas da Bitdefender partilham dicas e truques sobre como se protegerem contra hackers, violações de dados, roubo de identidade e tentativas de personificação social.

A página da Bitdefender Cyberpedia pode ser encontrada aqui:

https://www.bitdefender.com/cyberpedia/.

4.3. Informações de Contato

Uma comunicação eficiente é a chave para um negócio de sucesso. Desde 2001 a BITDEFENDER estabeleceu uma reputação inquestionável por buscar constantemente uma melhor comunicação para superar as expectativas de nossos clientes e parceiros. Se você tiver alguma dúvida, não hesite em nos contatar diretamente através do nosso Centro de Suporte da Bitdefender (página 22).

https://www.bitdefender.pt/consumer/support/

4.3.1. Distribuidores locais

Os distribuidores locais BitDefender estão preparados para responder a quaiquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor da Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha o seu país e cidade utilizando as opções correspondentes.

GLOSSÁRIO

Código de ativação

É um código exclusivo que pode ser comprado no varejo e usado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma assinatura válida por um determinado período de tempo e determinados dispositivos e também pode ser usado para estender uma assinatura com a condição de ser gerada para o mesmo produto ou serviço.

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam chamá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interativas que se parecem e se comportam como programas de computador, em vez de páginas estáticas. Com o ActiveX, os usuários podem fazer ou responder perguntas, usar botões de pressão e interagir de outras maneiras com a página da web. Os controles ActiveX geralmente são escritos usando o Visual Basic. Active X é notável por uma completa falta de controles de segurança; especialistas em segurança de computadores desencorajam seu uso pela internet.

Ameaça persistente avançada

Ameaça persistente avançada (APT) explora vulnerabilidades de sistemas para roubar informações importantes para entregá-las à fonte. Grandes grupos, como organizações, empresas ou governos, são alvo dessa ameaça. O objetivo de uma ameaça persistente avançada é permanecer indetectável por muito tempo, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas visadas. O método usado para injetar a ameaça na rede é por meio de um arquivo PDF ou documento do Office que pareça inofensivo para que todos os usuários possam executar os arquivos.

Adware

O adware geralmente é combinado com um aplicativo host fornecido gratuitamente, desde que o usuário concorde em aceitar o adware. Como os aplicativos de adware geralmente são instalados depois que o usuário concorda com um contrato de licenciamento que declara a finalidade do aplicativo, nenhuma ofensa é cometida. No entanto, anúncios pop-

up podem se tornar um aborrecimento e, em alguns casos, degradar o desempenho do sistema. Além disso, as informações que alguns desses aplicativos coletam podem causar problemas de privacidade para usuários que não estavam totalmente cientes dos termos do contrato de licença.

Arquivo

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um arquivo que contém um ou mais arquivos em um formato compactado.

Porta dos fundos

Uma brecha na segurança de um sistema deliberadamente deixada por designers ou mantenedores. A motivação para tais buracos nem sempre é sinistra; alguns sistemas operacionais, por exemplo, vêm com contas privilegiadas destinadas ao uso por técnicos de serviço de campo ou programadores de manutenção do fornecedor.

Setor de inicialização

Um setor no início de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster e assim por diante). Para discos de inicialização, o setor de inicialização também contém um programa que carrega o sistema operacional.

Vírus de inicialização

Uma ameaça que infecta o setor de inicialização de um disco fixo ou disquete. Uma tentativa de inicializar a partir de um disquete infectado com um vírus do setor de inicialização fará com que a ameaça se torne ativa na memória. Toda vez que você inicializar seu sistema a partir desse ponto, você terá a ameaça ativa na memória.

botnet

O termo “botnet” é composto pelas palavras “robô” e “rede”. Botnets são dispositivos conectados à Internet infectados com ameaças e podem ser usados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis ou espalhar spyware, ransomware e outros tipos de ameaças. Seu objetivo é infectar o maior número possível de dispositivos conectados, como PCs, servidores, dispositivos móveis ou IoT pertencentes a grandes empresas ou indústrias.

Navegador

Abreviação de navegador da web, um aplicativo de software usado para localizar e exibir páginas da web. Os navegadores populares incluem Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que eles podem exibir gráficos, bem como texto. Além disso, a maioria dos navegadores modernos pode apresentar informações multimídia, incluindo som e vídeo, embora exijam plug-ins para alguns formatos.

Ataque de força bruta

Ataque de adivinhação de senha usado para invadir um sistema de computador inserindo possíveis combinações de senha, geralmente começando com a senha mais fácil de adivinhar.

Linha de comando

Em uma interface de linha de comando, o usuário digita comandos no espaço fornecido diretamente na tela usando a linguagem de comando.

Biscoitos

Na indústria da Internet, os cookies são descritos como pequenos arquivos contendo informações sobre computadores individuais que podem ser analisados e usados por anunciantes para rastrear seus interesses e gostos online. Neste domínio, a tecnologia de cookies ainda está sendo desenvolvida e a intenção é direcionar os anúncios diretamente para o que você disse que são seus interesses. É uma faca de dois gumes para muitas pessoas porque, por um lado, é eficiente e pertinente, pois você só vê anúncios sobre o que está interessado. Por outro lado, envolve realmente "rastrear" e "seguir" onde você vai e o que você clicar. Compreensivelmente, há um debate sobre privacidade e muitas pessoas se sentem ofendidas com a noção de que são vistas como um "número SKU" (você sabe, o código de barras no verso dos pacotes que é escaneado na fila do caixa do supermercado) . Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.

Cyberbullying

Quando colegas ou estranhos estão cometendo atos abusivos contra crianças com o propósito de machucá-las fisicamente. Para prejudicar emocionalmente, os agressores estão enviando mensagens maldosas ou fotos pouco lisonjeiras, fazendo com que suas vítimas se isolem dos outros ou se sintam frustradas.

Ataque de dicionário

Ataques de adivinhação de senha usados para invadir um sistema de computador inserindo uma combinação de palavras comuns para gerar senhas em potencial. O mesmo método é usado para adivinhar as chaves de descriptografia de mensagens ou documentos criptografados. Os ataques de dicionário são bem-sucedidos porque muitas pessoas tendem a escolher senhas curtas e simples que são fáceis de adivinhar.

Unidade de disco

É uma máquina que lê e grava dados em um disco. Uma unidade de disco rígido lê e grava discos rígidos. Uma unidade de disquete acessa disquetes. As unidades de disco podem ser internas (alojadas em um computador) ou externas (alojadas em uma caixa separada que se conecta ao computador).

Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um dispositivo periférico. O termo é frequentemente usado para descrever o processo de copiar um arquivo de um serviço online para o próprio computador. O download também pode se referir à cópia de um arquivo de um servidor de arquivos de rede para um computador na rede.

E-mail

Correio eletrônico. Um serviço que envia mensagens em computadores através de redes locais ou globais.

Eventos

Uma ação ou ocorrência detectada por um programa. Os eventos podem ser ações do usuário, como clicar em um botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

Exploits

Uma forma de aproveitar diferentes bugs ou vulnerabilidades que estão presentes em um computador (software ou hardware). Assim, os hackers podem obter o controle de computadores ou redes.

Falso positivo

Ocorre quando um mecanismo de varredura identifica um arquivo como infectado quando, na verdade, não está.

Extensão de nome de arquivo

A parte de um nome de arquivo, após o ponto final, que indica o tipo de dados armazenados no arquivo. Muitos sistemas operacionais usam extensões de nome de arquivo, por exemplo, Unix, VMS e MS-DOS. Eles geralmente têm de uma a três letras (alguns sistemas operacionais antigos e tristes não suportam mais do que três). Os exemplos incluem "c" para código-fonte C, "ps" para PostScript, "txt" para texto arbitrário.

Heurística

Um método baseado em regras para identificar novas ameaças. Este método de verificação não depende de um banco de dados de informações de ameaças específico. A vantagem da verificação heurística é que ela não é enganada por uma nova variante de uma ameaça existente. No entanto, ocasionalmente pode relatar códigos suspeitos em programas normais, gerando o chamado "falso positivo".

Pote de mel

Um sistema de computador isca criado para atrair hackers para estudar a maneira como eles agem e identificar os métodos heréticos que usam para coletar informações do sistema. Empresas e corporações estão mais interessadas em implementar e usar honeypots para melhorar seu estado geral de segurança.

IP

Protocolo de Internet - Um protocolo roteável no conjunto de protocolos TCP/IP que é responsável pelo endereçamento IP, roteamento e fragmentação e remontagem de pacotes IP.

miniaplicativo Java

Um programa Java projetado para ser executado apenas em uma página da Web. Para usar um applet em uma página da web, você deve especificar o nome do applet e o tamanho (comprimento e largura, em pixels) que o applet pode utilizar. Quando a página é acessada, o navegador baixa o applet de um servidor e o executa na máquina do usuário (o cliente). Os applets diferem dos aplicativos porque são regidos por um protocolo de segurança estrito.

Por exemplo, embora os applets sejam executados no cliente, eles não podem ler ou gravar dados na máquina do cliente. Além disso, os applets são ainda mais restritos para que possam apenas ler e gravar dados do mesmo domínio do qual são servidos.

Keylogger

Um keylogger é um aplicativo que registra tudo o que você digita. Keyloggers não são maliciosos por natureza. Eles podem ser usados para fins legítimos, como monitorar atividades de funcionários ou crianças. No entanto, eles estão sendo cada vez mais usados por cibercriminosos para fins maliciosos (por exemplo, para coletar dados privados, como credenciais de login e números de CPF).

Vírus de macro

Um tipo de ameaça de computador codificada como uma macro incorporada a um documento. Muitos aplicativos, como Microsoft Word e Excel, oferecem suporte a poderosas linguagens de macro. Esses aplicativos permitem que você incorpore uma macro em um documento e execute a macro sempre que o documento for aberto.

cliente de e-mail

Um cliente de e-mail é um aplicativo que permite enviar e receber e-mails.

Memória

Áreas de armazenamento interno no computador. O termo memória identifica o armazenamento de dados que vem na forma de chips, e a palavra armazenamento é usada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente chamada de memória principal ou RAM.

Não heurístico

Este método de verificação depende de um banco de dados de informações de ameaças específico. A vantagem da verificação não heurística é que ela não é enganada pelo que pode parecer uma ameaça e não gera alarmes falsos.

predadores online

Indivíduos que procuram atrair menores ou adolescentes para conversas com o propósito de envolvê-los em atividades sexuais ilegais. As redes sociais são o local ideal onde crianças vulneráveis podem ser facilmente caçadas e induzidas a praticar atividades sexuais, online ou face a face.

Programas compactados

Um arquivo em um formato de compactação. Muitos sistemas operacionais e aplicativos contêm comandos que permitem compactar um arquivo para que ele ocupe menos memória. Por exemplo, suponha

que você tenha um arquivo de texto contendo dez caracteres de espaço consecutivos. Normalmente, isso exigiria dez bytes de armazenamento.

No entanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere de série de espaço especial seguido pelo número de espaços sendo substituídos. Nesse caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de empacotamento - existem muitas outras.

Caminho

As direções exatas para um arquivo em um computador. Essas direções geralmente são descritas por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre quaisquer dois pontos, como o canal de comunicação entre dois computadores.

Phishing

O ato de enviar um e-mail a um usuário que afirma falsamente ser uma empresa legítima estabelecida na tentativa de enganar o usuário para que entregue informações privadas que serão usadas para roubo de identidade. O e-mail direciona o usuário a visitar um site onde é solicitado que ele atualize as informações pessoais, como senhas e números de cartão de crédito, previdência social e contas bancárias, que a organização legítima já possui. O site, no entanto, é falso e criado apenas para roubar as informações do usuário.

Fóton

Photon é uma tecnologia inovadora não intrusiva da Bitdefender, concebida para minimizar o impacto da solução de segurança. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

Vírus polimórfico

Uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs e teclados.

Externamente, os computadores pessoais portas para ligar modems, impressoras, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ransomware

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem os sistemas pessoais dos utilizadores.

A infeção pode ser espalhada através do acesso a um e-mail de spam, transferência de anexos de e-mail ou da instalação de aplicações, sem que o utilizador saiba o que está a acontecer no seu sistema. Os utilizadores diários e as empresas são os alvos dos hackers ransomware.

Arquivo de relatório

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, são principalmente utilizados para ocultar ameaças ou esconder a presença de um intruso no sistema. Quando combinados com ameaças, os rootkits são uma grande ameaça à integridade e à segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Script

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. Geralmente atribuído a qualquer e-mail não solicitado.

Spyware

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

O spyware é similar a uma ameaça Cavalo de Troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens de inicialização

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã de arranque, um ficheiro de som a ser reproduzido quando o computador arranca, um calendário de lembretes ou aplicações podem ser itens de arranque. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Inscrição

Acordo de compra que dá ao utilizador o direito de utilizar um produto ou serviço específico num número específico de dispositivos e durante um período de tempo determinado. Uma subscrição expirada pode ser automaticamente renovada utilizando as informações fornecidas pelo utilizador na primeira compra.

Bandeja do sistema

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

Ameaça

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria das ameaças também se pode replicar. Todas as ameaças de computador são criadas pelo homem. Uma simples ameaça pode copiar-se várias vezes e é relativamente fácil de produzir. Mesmo uma simples ameaça é perigosa porque pode rapidamente utilizar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

Atualização de informações sobre ameaças

O padrão binário de uma ameaça é utilizado pela solução de segurança para detetá-la e eliminá-la.

Troiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário de programas de software maliciosos e worms, os Trojans não se replicam, mas podem ser igualmente destrutivos. Um dos tipos mais

insidiosos de ameaças de cavalo de Troia é um programa que afirma remover as ameaças do seu computador, mas, em vez disso, introduz ameaças no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Atualizar

Uma nova versão de um produto de software ou hardware concebida para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da atualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a atualização.

O Bitdefender tem a sua própria funcionalidade de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

Rede Privada Virtual (VPN)

É uma tecnologia que ativa uma conexão direta temporária e criptografada para uma certa rede sobre uma rede menos segura. Dessa forma, enviar e receber dados é seguro e criptografado, difícil de virar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com o uso de um nome de usuário e senha.

Worm

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.