GUIA DO UTILIZADOR

Bitdefender CONSUMER SOLUTIONS

Password Manager

Bitdefender Password Manager

Guia do usuário

Data de publicação 06/09/2023

Notícia legal

Bitdefender

Índice

SOBRE ESTE GUIA

Propósito e público-alvo

Este guia é destinado a todos os utilizadores da Bitdefender em todos os sistemas operacionais suportados (Windows, MacOS, Android, iOS) que escolheram Bitdefender Password Manager como sua ferramenta de gestão de palavras-passe de preferência. As informações apresentadas neste livro são adequadas não apenas para entendidos, mas também servem como um guia acessível e amigável para todos.

Este guia irá ajudá-lo a descobrir como fazer o melhor uso do nosso Gestor de Palavras-passe superseguro e rico em recursos, discutindo em detalhes todas as suas características e funcionalidades.

Desejamos-lhe uma leitura agradável e útil.

Como Utilizar Este Guia

Este manual está organizado em diversos tópicos importantes:

Começar (página 5)

Comece por Bitdefender Password Manager e o processo de instalação.

Características e Funcionalidades (página 20)

Aprenda a utilizar Bitdefender Password Manager e todas as suas funcionalidades.

Conseguindo ajuda (página 31)

Onde procurar e onde pedir ajuda se algo inesperado acontecer.

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. O QUE É BITDEFENDER PASSWORD MANAGER

Bitdefender Password Manager é um serviço multiplataforma projetado para ajudar os utilizadores a armazenar e organizar todas as suas palavras-passe online. Ele é desenhado com os algoritmos criptográficos mais fortes conhecidos para o mais alto nível de proteção e segurança digital. Funciona como uma extensão de navegador e uma solução de aplicação móvel para gestão de identidade e palavras-passe, bancos e todos os outros tipos de informações sensíveis através de dispositivos.

Bitdefender Password Manager pode guardar e preencher automaticamente, gerar e gerir as suas palavras-passe automaticamente para todos os sites e serviços online com a ajuda de uma única palavra-passe mestre, tornando a sua identidade digital muito mais fácil de gerir.

1.1. Segurança e como ela funciona

Por trás do software Bitdefender Password Manager estão alguns dos mais recentes algoritmos criptográficos que asseguram a mais avançada segurança de dados que os utilizadores poderiam querer, tais como protocolos AES-256-CCM, SH512, BCRYPT, HTTPS e WSS para transmissão de dados. Todos os dados envolvidos são sempre encriptados e desencriptados localmente. Isto faz com que apenas o titular da conta possa ter acesso às informações armazenadas dentro da conta, bem como à palavra-passe mestre que é utilizada para aceder e posteriormente utilizar os dados em questão.

1.2. Versões de teste e paga do Gestor de Palavras-passe

A versão de teste do Gestor de Palavras-passe da Bitdefender funciona igual à versão paga do produto em todos os sentidos, mas sua disponibilidade expirará após 90 dias de sua ativação.

> **Observação**
> Observe que embora a versão paga do produto possa ser adquirida como um produto por separado, o acesso ilimitado ao Gestor de Palavras-passe está incluído nas subscrições do Bitdefender Premium Security e Bitdefender Ultimate Security.

2. COMEÇAR

2.1. Requisitos de Sistema

Só pode utilizar a última versão do Bitdefender Password Manager em dispositivos que executem os seguintes sistemas operativos:

- **Para utilizadores de PC:**
  - Windows 7 com o Service Pack 1
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Para utilizadores de macOS:**
  - macOS 10.14 (Mojave) e sistemas operativos macOS posteriores

  Observação
  Saiba que o desempenho do sistema pode ser afetado em dispositivos com CPUs de geração antiga.
- **Para utilizadores de iOS:**
  - iOS 11.0 ou sistemas operativos iOS posteriores
- **Para utilizadores de Android:**
  - Android 5.1 ou sistemas operativos Android posteriores

  Observação
  - A funcionalidade de desbloqueio por impressão digital é suportada no **Android 6.0** e posterior.
  - A funcionalidade de Preenchimento automático é suportada no **Android 8.0** e superior, compatível com iPhone, iPad e iPod touch.

2.1.1. Requisitos de Software

Para conseguir utilizar o Bitdefender Password Manager e todas as suas funcionalidades, os seus dispositivos Windows ou MacOS precisam atender aos seguintes requisitos de software:

- **Microsoft Edge** (baseado em Chromium 80 e posteriores)
- **Mozilla Firefox** (versão 65 ou posterior)
- **Google Chrome** (versão 72 ou posterior)
- **Safari** (versão 12 ou posterior)

Observação

Os requisitos de Software não são aplicáveis para Android e iOS.

Aviso

O incumprimento dos Requisitos do Sistema apresentados acima resultará na incapacidade de instalar o Bitdefender Password Manager ou na avaria do produto.

2.2. Instalação

Este capítulo irá guiá-lo sobre como instalar o Bitdefender Password Manager tanto nos navegadores web no seu PC Windows e MacOS, como também nos seus dispositivos móveis Android ou iOS.

Importante

Antes da instalação, certifique-se de ter uma subscrição válida do Password Manager na sua conta da **Central Bitdefender** para que esta extensão do navegador possa recuperar a validade da sua conta.

As subscrições ativas estão listadas na seção **As minhas Subscrições** dentro da Central Bitdefender.

2.2.1. Instalando em dispositivos Windows e macOS

Ao contrário da maioria das aplicações de ambiente de trabalho e software que precisam ser instalados e configurados nestes dispositivos, o Bitdefender Password Manager vem como uma extensão do navegador - também chamado de suplemento - que pode ser rapidamente adicionado e ativado no seu navegador preferido.

Os browsers atualmente suportados para o produto são os seguintes: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge**, e **Safari**.

1. Vá para https://central.bitdefender.com/ e inicie sessão na sua conta. Se ainda não tem uma conta, clique em **CRIAR CONTA** e, em seguida, introduza o seu nome completo, um endereço de e-mail e uma palavra-passe.
2. Selecione **Os meus dispositivos** na barra lateral esquerda do ecrã.
3. Na secção **Os meus dispositivos**, prossiga ao clicar em **+ Adicionar Dispositivo**.
4. Esta ação fará com que surja uma nova janela. Escolha **Password Manager** no ecrã de seleção.
5. Escolha **Este dispositivo**.
   Se estiver a procurar instalar num dispositivo diferente, selecione Outros dispositivos. Então, pode enviar uma ligação de transferência por e-mail para o dispositivo correspondente ou copiar diretamente o URL para a instalação.
6. Em seguida, escolha em que browser deseja instalar a extensão do Password Manager.
7. Cada botão correspondente irá redirecioná-lo para a Loja de Extensões do navegador. A partir daí, basta seguir as instruções no ecrã como mostrado abaixo:

   Microsoft Edge

   - Clique no botão **Obter**
   - Clique em **Adicionar extensão** no pedido que aparece no ecrã

   Google Chrome

   - Clique no botão **Adicionar ao Chrome**
   - Na caixa de confirmação, clique em **Adicionar extensão**

   Mozilla Firefox

   - Clique no botão **Adicionar ao Firefox**
   - Clique no botão **Instalar** no canto superior direito do ecrã

   Safari

   - Clique no botão **Obter** e, em seguida, clique em **Instalar**
   - Abra o Safari e selecione **Preferências** na barra de menu superior

- Na janela de Preferências, clique no separador **Extensões**
- Selecione a caixa de seleção ao lado do Password Manager para o ativar

Depois de ter seguido estes passos, defina uma palavra-passe mestre forte e, em seguida, pressione o botão **Guardar palavra-passe mestre** após ler e concordar com os **Termos e condições**.

Importante

Observe que precisará desta palavra-passe mestre para desbloquear todas as palavras-passe, informações de cartão de crédito e notas guardadas no Bitdefender Password Manager. Esta é basicamente a chave que permite ao proprietário utilizar este produto.

Aviso

Ao criar a palavra-passe mestre, receberá uma **chave de recuperação de 24 dígitos**. **Anote a sua chave de recuperação num lugar seguro e não a perca**. Esta chave é a única maneira de aceder às suas palavras-passe guardadas no Password Manager caso se **esqueça da palavra-passe mestre** previamente configurada para a sua conta.

- Pode premir **Fechar** quando tiver terminado.

2.2.2. Como instalar em dispositivos Android

O método mais fácil de instalar o Bitdefender Password Manager para telefones e tablets Android é transferir a aplicação diretamente do Google Play.

A instalação da aplicação Bitdefender Password Manager também pode ser feita através da sua conta da **Central Bitdefender**:

1. No seu dispositivo móvel Android, inicie sessão na sua conta da Central Bitdefender ao aceder a https://login.bitdefender.com/central/login.
2. Selecione **Meus dispositivos** na barra lateral esquerda da tela.
3. No **Meus dispositivos** seção, prossiga clicando em **+ Adicionar dispositivo**.

4. Esta ação abrirá uma nova janela. Escolher **Gerenciador de Senhas** na tela de seleção.
5. Escolher **Este aparelho**.
   Se estiver a procurar instalar num dispositivo diferente, selecione **Outros dispositivos**. Então, pode enviar uma ligação de transferência por e-mail para o dispositivo correspondente ou copiar diretamente o URL para a instalação.
6. Será redirecionado para o **Google Play**. Toque em **Instalar** para transferir o Bitdefender Password Manager no Android.
7. Uma vez terminada a transferência, abra a aplicação do Password Manager.
8. Se não for automaticamente ligado à sua conta, inicie sessão utilizando o seu nome de utilizador e palavra-passe.
   Depois de seguir essas etapas, defina uma senha mestra forte e pressione o botão **Salvar Senha Mestra** botão depois de ler e concordar com os **Termos e Condições**.

   Importante
   Observe que você precisará desta Senha Mestra para desbloquear todas as senhas, informações de cartão de crédito e notas salvas no Bitdefender Password Manager. Esta é essencialmente a chave que permite ao proprietário usar este produto.

   Aviso
   Ao criar a Senha Mestra, você receberá um **Chave de recuperação de 24 dígitos**. Anote sua chave de recuperação em um local seguro e não a perca. Esta chave é a única maneira de acessar suas senhas salvas no Gerenciador de Senhas caso você **esquecer a senha mestra** previamente configurado para sua conta.

   - você pode pressionar **Fechar** quando terminar.
9. Crie um **PIN de 4 dígitos**, portanto, se mudar para outra aplicação e, em seguida, regresse ao Password Manager, não terá que introduzir novamente a palavra-passe mestre que configurou anteriormente. Se disponível, também pode ativar o reconhecimento facial ou a autenticação de impressão digital.

10. Toque em **Preenchimento automático** para configurar as definições do preenchimento automático do Android.

> **Observação**
> Se ignorar este passo, pode ativar e personalizar as funcionalidades de preenchimento automático do Android posteriormente, seguindo as instruções disponíveis no Preenchimento automático inteligente (página 21).

11. Aparecerá uma lista de aplicações que podem preencher automaticamente as suas palavras-passe.
Selecione o **Password Manager** e, em seguida, o dispositivo irá pedir-lhe para confirmar que confia nesta aplicação.
Toque em **OK**.

12. Digite o PIN que configurou no **passo 9** para confirmar esta ação.

A instalação no seu dispositivo Android está agora completa.

2.2.3. Como instalar em dispositivos iOS

O método mais fácil de instalar o Bitdefender Password Manager em dispositivos iOS e iPadOS é transferir a aplicação diretamente da Apple App Store.

A instalação do aplicativo Bitdefender Password Manager também pode ser feita através do seu Bitdefender Central conta:

1. No seu iPhone ou iPad, inicie sessão na sua conta da Central Bitdefender ao aceder a https://login.bitdefender.com/central/login.
2. Selecione **Meus dispositivos** na barra lateral esquerda da tela.
3. No **Meus dispositivos** seção, prossiga clicando em **+ Adicionar dispositivo**.
4. Esta ação abrirá uma nova janela. Escolher **Gerenciador de Senhas** na tela de seleção.
5. Escolher **Este aparelho**.

Se você deseja instalar em um dispositivo diferente, selecione **Outros dispositivos**. Você pode enviar um link de download por e-mail para o respectivo dispositivo ou copiar diretamente o URL para a instalação.

6. Será redirecionado para a **App Store**. Toque no ícone da nuvem com uma seta apontada para baixo para transferir o Bitdefender Password Manager para iOS.
7. Uma vez instalada a aplicação , abra-a e verifique a pequena caixa no ecrã. Selecione **Continuar** depois de ler e concordar com o **Contrato de Subscrição**.
8. Se você não estiver conectado automaticamente à sua conta, faça login usando seu nome de usuário e senha.
   Depois de seguir essas etapas, defina uma senha mestra forte e pressione o botão **Salvar Senha Mestra** botão depois de ler e concordar com os **Termos e Condições**.

   Importante
   Observe que você precisará desta Senha Mestra para desbloquear todas as senhas, informações de cartão de crédito e notas salvas no Bitdefender Password Manager. Esta é essencialmente a chave que permite ao proprietário usar este produto.

   Aviso
   Ao criar a Senha Mestra, você receberá um **Chave de recuperação de 24 dígitos**. Anote sua chave de recuperação em um local seguro e não a perca. Esta chave é a única maneira de acessar suas senhas salvas no Gerenciador de Senhas caso você **esquecer a senha mestra** previamente configurado para sua conta.

   - você pode pressionar **Fechar** quando terminar.
9. Criar uma **PIN de 4 dígitos**, portanto, se você alternar para outro aplicativo e retornar ao Gerenciador de Senhas, não precisará inserir novamente a senha mestra que configurou anteriormente. Se disponível, você também pode habilitar o reconhecimento facial ou a autenticação de impressão digital.

A instalação no seu dispositivo iOS/iPadOS está agora completa.

3. PLANO COMPARTILHADO

O Bitdefender Password Manager Shared Plan permite que vários utilizadores acedam e utilizem a mesma subscrição. Fornece uma abordagem centralizada ao acesso, administração e suporte do software, oferecendo uma solução económica para partilhar o serviço de gestão de palavras-passe entre vários utilizadores.

- A pessoa responsável pelo plano de subscrição partilhada, conhecida como Gestor do Plano, pode partilhar o serviço entre os membros.
- Cada membro obtém a sua própria conta única Bitdefender Central ligada ao seu endereço de e-mail e acesso ao serviço Password Manager.

3.1. Compartilhando o Bitdefender Password Manager com vários usuários

Convidar membros

Para adicionar um ou vários usuários à assinatura compartilhada, o gestor do plano deve seguir estas etapas:

1. Inicie sessão na sua conta Bitdefender Central em https://central.bitdefender.com/.
2. Vá para o menu **As minhas subscrições** localizado no lado esquerdo da página.
3. Escolha **Convidar membro** no painel **Bitdefender Password Manager Shared Plan**.
4. Digite o e-mail de cada pessoa com quem deseja compartilhar sua assinatura e clique em **Enviar**. No máximo 3 membros podem ser adicionados de uma vez.
5. As instruções de configuração são enviadas imediatamente por correio eletrónico para os novos membros. Clique em **Fechar** para sair da janela de confirmação.

Observação

Os membros têm 24 horas para aceitar seu convite assim que ele for enviado a eles por e-mail.

- Os membros convidados aparecerão com o status “Convidado”.
- Você os verá como membros “ativos” depois que aceitarem o convite. Você também será notificado por e-mail sobre cada convite aceito.

Remover membros

O acesso ao Plano Partilhado do Bitdefender Password Manager é perdido para os membros que são removidos. Quando o gestor do plano decide remover um membro da subscrição, o membro recebe uma notificação por e-mail. Durante os 30 dias seguintes, o ex-membro é transferido para uma versão de avaliação de 30 dias do Bitdefender Password Manager com todas as capacidades. O serviço será então desativado.

O gestor do plano pode eliminar usuários do plano compartilhado da seguinte forma:

1. Faça login na sua conta Bitdefender Central em https://central.bitdefender.com/.
2. Vá para o menu **As minhas subscrições** localizado no lado esquerdo da página.
3. No painel **Bitdefender Password Manager Shared Plan** clique em **Gerir**, depois escolha **Editar membros** no menu.
4. Clique no botão **Remover** para retirar um membro do plano partilhado.
5. Escolha **Sim, remover membro** e clique no botão **Concluir edição** para que as alterações tenham efeito.

Observação

Quando um membro é eliminado do plano partilhado, o seu estado é alterado para **Remoção pendente** até ser completamente eliminado.

Aceitar um convite

Você receberá um e-mail quando alguém o convidar para se tornar um membro do Plano Compartilhado do Bitdefender Password Manager. Você tem 24 horas para aceitar um convite assim que ele for enviado a você.

Para aceitar o convite e ter acesso aos recursos do gerenciador de senhas, o usuário deve seguir estes passos:

1. Abra o e-mail que recebeu com o título **[Comece a utilizar a sua subscrição Bitdefender como Membro]** e clique no botão **ACTIVAR EM CENTRAL**.
2. A página do Bitdefender Central será então aberta no seu navegador.
   - Se já tiver uma conta de utilizador Bitdefender associada ao e-mail para o qual o convite foi enviado, **inicie sessão** para reclamar a sua subscrição partilhada.
   - Se não tiver uma conta de utilizador Bitdefender, clique em **Criar uma** e inscreva-se com o mesmo e-mail para o qual o convite foi enviado para reclamar a sua subscrição partilhada.
     - Introduza o seu nome completo
     - Introduza o seu endereço de e-mail
     - Introduza a sua palavra-passe
     - Clique no botão Criar conta e será assinado.
3. Depois de iniciar sessão, clique em **Começar** no ecrã de boas-vindas que o informa de que a sua subscrição do Bitdefender Password Manager está agora ativa.
4. Siga as etapas na tela também descritas em Instalação (página 6).

> **Observação**
> O e-mail do gerente do plano é exibido na sua conta Bitdefender Central na parte superior do menu do Gerenciador de Senhas e no cartão de assinatura, em Minhas Assinaturas.
>
> Se precisar de ajuda com o plano compartilhado, entre em contato com eles.

4. A IMPORTAR E EXPORTAR AS SUAS PALAVRAS-PASSE

O Bitdefender Password Manager está concebido de forma a facilitar a comunicação e transferência de dados com fontes externas, plataformas e ferramentas de software de forma eficiente. Esta é a principal razão pela qual a necessidade muito frequente de importar ou exportar palavras-passe para dentro ou fora do Bitdefender Password Manager pode ser satisfeita com facilidade.

4.1. Compatibilidade

O Bitdefender Password Manager pode facilmente transferir dados da seguinte lista de aplicações:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**

- **LastPass**
- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Observação**
> Se o nome do navegador ou da ferramenta de gestão de palavras-passe da qual está a tentar transferir ficheiros de dados não aparecer na lista fornecida acima, pode seguir o nosso guia online sobre como os utilizadores podem editar um ficheiro CSV de gestores de palavras-passe não suportados para importar as suas informações para o **Bitdefender Password Manager**: https://www.bitdefender.pt/consumer/support/answer/28156/

Esta transferência de dados entre o Bitdefender Password Manager e outros tipos de software de gestão de contas pode ser feita através dos seguintes formatos de dados:

CSV, **JSON**, **XML**, **TXT**, **1pif** e **FSK**.

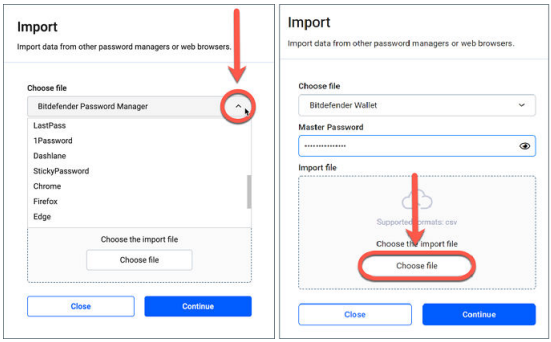
4.2. Importação para o Password Manager

O Bitdefender Password Manager permite importar facilmente palavras-passe de outros gestores de palavras-passe e navegadores. Se estiver a pensar em mudar para o Bitdefender Password Manager desde outro serviço de gestão de palavras-passe, é muito provável que tenha armazenado uma quantidade considerável de credenciais como nomes de utilizador, palavras-passe e outros dados de início de sessão necessários para todas as suas contas.

Agora que escolheu o Bitdefender Password Manager, deve importar os dados guardados para ele.

Veja aqui como importar as suas informações armazenadas de outras aplicações e navegadores web para o Bitdefender Password Manager, **independentemente do sistema operativo** no qual escolheu instalar este produto:

1. Clique no ícone do Password Manager no seu navegador web (no Windows ou macOS) ou inicie a aplicação do Password Manager (no Android ou iOS). Se solicitado, introduza a sua **Palavra-passe mestre**.
2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Definições**.
3. Desloque-se para baixo até à secção **Dados** e clique na opção **Importar dados**.
4. Utilize o menu de lista pendente para selecionar o nome da aplicação do Password Manager ou o navegador do qual deseja importar as suas contas. Introduza a sua **Palavra-passe mestre** no campo correspondente e, em seguida, clique em **Escolher Ficheiro**.



5. Navegue pelas suas pastas para encontrar o local onde guardou o ficheiro contendo os seus nomes de utilizador e palavras-passe, exportado do seu outro Password Manager ou navegador da web e, em seguida, pressione **Continuar**.

Uma vez importadas, as suas palavras-passe estarão acessíveis em todos os dispositivos onde a aplicação Bitdefender Password Manager ou extensão do navegador estiver instalada.

4.3. A exportar do Password Manager

O Bitdefender Password Manager permite-lhe exportar facilmente as suas palavras-passe guardadas (incluindo credenciais de início de sessão de

conta, notas seguras, etc.) para um ficheiro CSV (valores separados por vírgula) ou um ficheiro encriptado se quiser mudar para outro serviço de gestão de palavras-passe, para que a sua saída do Bitdefender Password Manager não seja um processo difícil.

> **Importante**
> Os ficheiros CSV **não** estão encriptados e contêm nomes de utilizador e palavras-passe em formato de texto simples, o que significa que as suas informações privadas podem ser lidas por qualquer pessoa que tenha acesso ao seu dispositivo. Portanto, recomendamos que siga as instruções abaixo num dispositivo confiável.

Veja aqui como pode exportar os seus dados do Bitdefender Password Manager:

1. Clique no ícone do Gerenciador de Senhas em seu navegador da Web (no Windows ou macOS) ou inicie o aplicativo Gerenciador de Senhas (no Android ou iOS). Se solicitado, digite seu Senha mestra.
2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Definições**.
3. Desloque-se para baixo até à secção **Dados** e clique na opção **Exportar dados**.
4. Agora deve poder ver as duas seguintes opções:
   - **CSV**
   - **Ficheiros protegidos por palavra-passe**

   Selecione a sua opção preferida e, em seguida, introduza a sua Palavra-passe mestre e clique no botão **Exportar dados**.

   > **Observação**
   > Se escolher a opção de ficheiro protegido por palavra-passe, será solicitado a encriptar os dados que contêm a lista de contas com uma palavra-passe, de forma que apenas você poderia acedê-lo se necessário.

5. O seu navegador da web/aplicação procederá a guardar um ficheiro chamado Bitdefender Password Manager_exported_data_current-date no seu sistema na pasta de transferência padrão. Ele contém todos os seus dados armazenados no Bitdefender Password Manager.

Após exportar os seus dados, pode carregá-los no Password Manager da sua escolha.

5. CARACTERÍSTICAS E FUNCIONALIDADES

Este capítulo explica todas as características e funcionalidades do Bitdefender Password Manager, a sua utilidade e como as operar da forma mais eficiente possível.

5.1. Tratamento de palavras-passe

5.1.1. Gerador de Palavras-passe

A regra de ouro em relação à segurança online é utilizar sempre frases aleatórias exclusivas para cada serviço que requer a criação de uma conta. A reutilização de palavras-passe em múltiplas plataformas é o motivo número um por trás do roubo de identidade e das perdas associadas ao roubo de contas.

Esta funcionalidade ajuda os utilizadores a gerar palavras-passe seguras, complexas e exclusivas para cada nova conta que eles criarem em qualquer lugar online. Isto elimina a necessidade dos utilizadores terem que criar palavras-passe fortes por conta própria ou terem cuidado para não reutilizar a mesma palavra-passe para várias contas.

O **Gerador de Palavras-passe** pode ser acedido através do separador na parte superior da interface do Password Manager.

O gerador pode ser configurado para gerar palavras-passe **entre 4 e 32 caracteres**.

Também pode especificar os tipos de caracteres que devem ou não estar presentes na palavra-passe gerada aleatoriamente, marcando ou desmarcando as caixas de seleção correspondentes. **(Letra minúscula, letra maiúscula, números, especial)**

Ao premir o botão ↻ à direita da palavra-passe exibida, o gerador irá alterar a palavra-passe sugerida.

Para utilizar a palavra-passe exibida, pressione **Utilizar palavra-passe**, ação que guardará a sequência de caracteres na sua área de transferência.

> **Observação**
> As suas palavras-passe geradas anteriormente serão temporariamente armazenadas no Histórico de palavras-passe, que pode ser acedido através do botão **Histórico de palavras-passe**.

5.1.2. Captura de palavras-passe

Com esta funcionalidade do Password Manager, deverá armazenar todas as suas novas palavras-passe imediatamente após a criação das mesmas. O Password Manager solicitará aos utilizadores que armazenem as suas palavras-passe recém-criadas, para que elas possam ser adicionadas imediatamente ao ambiente superseguro fornecido pela Bitdefender.

5.1.3. Preenchimento automático inteligente

O Bitdefender Password Manager pode ser configurado de forma que ele possa preencher automaticamente suas credenciais de início de sessão e, mais importante, as suas palavras-passe. Algoritmos patenteados podem detectar e pré-preencher credenciais em sites previamente visitados, poupando o tempo dos utilizadores sempre que eles iniciarem sessão num serviço.

1. No Windows ou macOS, clique no ícone **Password Manager** no seu navegador web.

   No Android ou iOS, abra a aplicação do **Password Manager**.
   Se solicitado, introduza a sua **Palavra-passe mestre**.

2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Definições**.
3. Clique em **Definições do dispositivo**.
4. Aqui notará um botão exibindo **Desativar preenchimento automático** ou **Ativar preenchimento automático**. Esta definição controla o estado operacional da funcionalidade de preenchimento automático inteligente.

5.1.4. Relatório de Segurança

O Relatório de Segurança é uma ferramenta que irá gerar relatórios baseados numa série de características destinadas a reforçar sua segurança digital. Ele informará se uma senha requer sua atenção

imediata, determinando o seu nível de segurança. Ele detecta palavras-passe duplicadas e recomenda mudá-las, evitando os perigos de reciclar as mesmas palavras-passe para várias contas.

O relatório concentra-se em fornecer informações sobre a higiene geral de palavras-passe, no que se refere a palavras-passe duplicadas, palavras-passe fracas ou violadas ou endereços de e-mail.

Isso é feito comparando a lista de hashes encriptados da página web de Troy localmente no seu dispositivo para verificar se ele contém os hashes correspondentes de suas palavras-passe. Se for encontrada alguma correspondência, será notificado para alterar as suas palavras-passe e outras credenciais de início de sessão.

Para aceder ao **Relatório de segurança**, aceda a interface do Password Manager e selecione o botão correspondente na barra superior.

5.1.5. Sincronização através de outras plataformas

Ao guardar as suas palavras-passe uma vez no Bitdefender Password Manager, poderá armazená-las e acedê-las com segurança em todos os seus dispositivos Windows, Mac, Android ou iOS a partir do Chrome, Safari, Firefox e Edge ou dentro de aplicações móveis.

> **Observação**
> A Bitdefender também está equipada com um **modo offline** para aceder às suas palavras-passe, caso não tenha acesso à internet. Isso torna suas palavras-passe acessíveis em qualquer momento e em qualquer lugar.

5.1.6. Eliminar uma entrada

Para eliminar palavras-passe , primeiro pressione o ícone de editar ao lado do registro que deseja remover, localizado no separador **Contas**. Role para baixo e escolha **Eliminar**. Ao ser perguntado se tem a certeza de querer remover a conta, selecione **Remover**.

5.2. Tratamento de contas

5.2.1. Autenticação

A autenticação no Bitdefender Password Manager é feita através do **PIN** configurado no processo de instalação do produto. (Note que a

funcionalidade de **Bloqueio automático** bloqueará ou sairá do Password Manager após um período de inatividade no navegador ou fechará a aplicação móvel)

Além disso, também pode ser feito através de biometria, se disponível, como a **Impressão digital** ou o **Desbloqueio facial**.

Para **ativar ou desativar** a autenticação por biometria:

1. No Windows ou macOS, clique no botão **Password Manager** ícone em seu navegador da web.

   No Android ou iOS, inicie o **Password Manager** aplicativo.
   Se solicitado, digite seu Senha mestra.

2. Abra o menu Gerenciador de Senhas para expandir a barra lateral à esquerda e clique no botão **Configurações** item do menu.
3. Clique em **Configurações do dispositivo**.
4. Aqui verá um botão exibindo **Desativar biometria** ou **Ativar biometria**. Esta definição controla o estado operacional da funcionalidade de autenticação por biometria.

5.2.2. Redefinição da palavra-passe mestre

> **Importante**
> A funcionalidade **Alterar palavra-passe mestre** não está disponível nos dispositivos móveis. A única maneira de alterar ou recuperar a sua palavra-passe mestre é através da extensão do navegador Bitdefender Password Manager num PC Windows ou num dispositivo MacOS.

Veja aqui como alterar a sua **Palavra-passe mestre** como medida de precaução e crie uma nova palavra-passe no Bitdefender Password Manager:

1. No Windows ou macOS, clique no ícone do **Password Manager** na barra de ferramentas do seu navegador web.
2. Introduza a sua palavra-passe mestre atual para desbloquear o cofre.

> **Importante**
> Se não se lembra da palavra-passe mestre atual, clique na opção **Esqueci a minha palavra-passe** no mesmo ecrã. Digite os **24 dígitos da chave de recuperação** fornecida durante a configuração inicial do Bitdefender Password Manager e, em seguida, digite uma nova palavra-passe mestre. **Se esquecer ou perder** tanto a **Palavra-passe mestre** como a **Chave de recuperação**, como último recurso, **contacte um representante da Bitdefender para ajudar a repor a sua conta**. A reposição da sua conta irá **eliminar todos os seus dados e palavras-passe** guardados no Bitdefender Password Manager.

3. Abra o menu Gerenciador de Senhas para expandir a barra lateral à esquerda e clique no botão **Configurações** item do menu.
4. Clique no botão **A minha conta** na secção **Conta**.
5. Uma janela com informações sobre sua subscrição do Password Manager será exibida.
   Clique no botão **Alterar palavra-passe mestre**.
6. Será redirecionado para uma nova janela onde poderá escolher uma nova palavra-passe mestre. Introduza a sua palavra-passe mestre atual e, em seguida, introduza uma nova palavra-passe mestre. A nova palavra-passe mestre deve conter no mínimo 8 caracteres, pelo menos uma letra minúscula, uma letra maiúscula e um número.
7. Pressione o botão **Alterar** quando tiver terminado.
8. Espere alguns momentos até que o Bitdefender restabeleça a antiga palavra-passe mestre.
   Não saia do seu navegador da web!
9. Em seguida, receberá uma chave de recuperação nova de **24 dígitos**. Anote a sua chave de recuperação num lugar seguro **e não a perca**. Esta chave é a única maneira de aceder às suas palavras-passe guardadas no Password Manager caso se esqueça da palavra-passe mestre.
   Pode pressionar **Fechar** quando tiver terminado.
10. Será desconectado do Bitdefender Password Manager.
    Para desbloquear o cofre, utilize a palavra-passe mestre nova que acabou de definir.

5.3. Outras funcionalidades

5.3.1. Gestão de identidades

Esta funcionalidade permite que os utilizadores armazenem múltiplas identidades e que o Password Manager preencha automaticamente os detalhes em formulários da web antes de fazer uma compra de forma rápida, fácil e segura.

Como todo o resto no Password Manager, todos os dados sensíveis contidos nestas identidades armazenadas são encriptados e disponíveis apenas no dispositivo do utilizador.

Para adicionar uma identidade ao Password Manager:

1. No Windows ou macOS, clique no botão **Password Manager** ícone em seu navegador da web.

   No Android ou iOS, inicie o **Password Manager** aplicativo.
   Se solicitado, digite seu Senha mestra.

2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Identidades**.
3. Prima o botão **Adicionar identidade** na parte inferior.
4. Complete os detalhes que deseja armazenar e prima **Guardar**.

5.3.2. Gestão do cartão de crédito

Esta funcionalidade permite guardar e preencher detalhes do cartão de crédito para compras de forma mais fácil, rápida e segura.

Para adicionar um cartão de crédito ao Password Manager:

1. No Windows ou macOS, clique no botão **Password Manager** ícone em seu navegador da web.

   No Android ou iOS, inicie o **Password Manager** aplicativo.
   Se solicitado, digite seu Senha mestra.

2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Cartões de crédito**.
3. Pressione o **Adicionar identidade** botão na parte inferior.
4. Complete os detalhes que você deseja armazenar e pressione **Salvar**.

5.3.3. Secure Me

O recurso Secure Me permite que saia ou exclua remotamente o histórico de navegação do seu computador, tablet ou dispositivo móvel. Se estiver a partilhar um dispositivo com outras pessoas, recomendamos fortemente que ative este recurso.

Para localizar e ativar esta funcionalidade:

1. No Windows ou macOS, clique no botão **Password Manager** ícone em seu navegador da web.
   No Android ou iOS, inicie o **Password Manager** aplicativo.
   Se solicitado, digite seu Senha mestra.
2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Secure Me**.
3. Pressione o botão **Proteger todas as sessões**.
   Se deseja proteger apenas um determinado dispositivo, procure-o na lista de dispositivos no qual o Password Manager está instalado ou ativado num navegador específico.

5.3.4. Notas

O Secure Notes atua como um caderno secreto no qual pode armazenar dados sensíveis, classificá-los e codificá-los por cores para visualizá-los melhor. Isso não só mantém as informações organizadas, mas também as mantém seguras e protegidas.

Para localizar e habilitar esse recurso:

1. No Windows ou macOS, clique no botão **Password Manager** ícone em seu navegador da web.
   No Android ou iOS, inicie o **Password Manager** aplicativo.
   Se solicitado, digite seu Senha mestra.
2. Abra o menu do Password Manager para expandir a barra lateral à esquerda e clique no item do menu **Notas**.
3. Pressione o botão **Adicionar nota**.
   Após anotar as informações que deseja guardar em segurança, prima **Guardar**.

6. PERGUNTAS FREQUENTES

Algumas perguntas comuns sobre o Bitdefender Password Manager tendem a se repetir. Nós temos as respostas! Aqui pode saber mais sobre a sua conta Bitdefender, importação de palavras-passe, protocolos de segurança de dados e outros tópicos importantes para nossos clientes.

Perguntas gerais sobre o Bitdefender Password Manager

Como posso parar o pop-up do Password Manager na minha solução de segurança Bitdefender?

A notificação do Password Manager exibida pelo Bitdefender Total Security, Internet Security e Antivirus Plus em agosto de 2022 pode ser descartada ao clicar no botão “x”. A janela “Gerir palavras-passe com o Bitdefender Password Manager” irá reaparecer aleatoriamente algumas vezes antes de desaparecer para sempre. Pode optar por não ver esta mensagem promocional ao desativar as **Notificações de recomendação** nas Configurações do Bitdefender.

O que acontece quando o Bitdefender Password Manager expira?

Quando a sua subscrição do Password Manager expirar e não estiver mais ativa, terá um máximo de 90 dias para exportar as suas palavras-passe. As suas palavras-passe serão armazenadas por mais 30 dias. Durante estes 90 dias, apenas poderá exportar os seus dados. Não poderá continuar a utilizar o Password Manager. O recurso de preenchimento automático deixará de funcionar, assim como a capacidade de gerar palavras-passe.

No final do período de 90 dias, terá 30 dias extras para entrar em contacto com o apoio ao cliente da Bitdefender e solicitar a restauração das suas palavras-passe de volta para o banco de dados em tempo real. Então, poderá exportar as suas palavras-passe do Bitdefender Password Manager.

Os seus dados serão mantidos na base de dados em tempo real apenas até ao final do dia em que forem restaurados a pedido. À meia-noite, a base de dados é apagada – e se ainda não tiver ultrapassado o período adicional de 30 dias, as palavras-passe podem ser restauradas novamente a partir da cópia de segurança. Os dados brutos da base de

dados da cópia de segurança podem ser fornecidos a pedido do utilizador, no entanto, a base de dados é encriptada e não é possível aceder às informações.

O que é uma palavra-passe mestre e porque é que tenho de me lembrar dela?

A palavra-passe mestre é a chave que abre a porta para todas as palavras-passe armazenadas na sua conta do Bitdefender Password Manager. A palavra-passe mestre deve possuir no mínimo 8 caracteres. Portanto, crie uma palavra-passe mestre forte, memorize-a e nunca a partilhe com ninguém. Para criar uma palavra-passe segura, recomendamos a utilização de uma combinação de maiúsculas e minúsculas, números e caracteres especiais (como, $, ou @).

Como posso impedir a Bitdefender de pedir a minha palavra-passe mestre sempre que abro o navegador?

Se bloquear o seu dispositivo sem fechar o browser, o Password Manager não bloqueia, sendo que pode ter acesso aos seus dados quando regressar. Como medida de segurança, sempre que abrir o browser, terá de iniciar sessão na sua conta da Central Bitdefender e depois introduzir a sua palavra-passe principal.

- Para interromper a solicitação de início de sessão na Central, aceda as Definições e marque “Desativar o separador de início de sessão no arranque”.
- Para interromper a mensagem da palavra-passe principal, marque a caixa “Lembrar-me” no ecrã Desbloquear o seu cofre.

Porque é que não guarda a minha Palavra-passe mestre, e o que acontece se eu a esquecer?

A razão pela qual não armazenamos a sua Palavra-passe mestre em nossos servidores é para que apenas o dono da conta possa aceder à sua conta. É a forma mais segura. Se o Bitdefender Password Manager não reconhecer a sua Palavra-passe mestre, certifique-se de que está a introduzi-la corretamente e que a tecla Caps Lock não está ativa no teclado.

Caso se esqueça da sua palavra-passe principal, pode utilizar a Chave de Recuperação para desbloquear o Password Manager. Durante o processo de registo, o Bitdefender Password Manager fornece uma **chave de recuperação** que pode ser utilizada para recuperar o acesso à conta sem perder os seus dados.

Se esquecer ou perder a palavra-passe mestre e a chave de recuperação, como último recurso, entre em contacto com um representante da Bitdefender para repor a sua conta.

> **Importante**
> A reposição da sua conta apagará todos os seus dados e palavras-passe guardados no Bitdefender Password Manager.

Vários utilizadores podem partilhar uma subscrição do Bitdefender Password Manager?

Por enquanto, a possibilidade de ter vários utilizadores na mesma subscrição do Password Manager não está disponível, mas estamos trabalhando para ativar esta funcionalidade num futuro próximo.

O que é o modo Offline e como é que funciona?

O modo offline é ativado automaticamente quando se perde a ligação à Internet durante a utilização do Bitdefender Password Manager. Se já tiver sessão iniciada e tiver introduzido a sua palavra-passe principal, o modo Offline permite-lhe aceder às suas palavras-passe quando não tiver ligação à Internet.

Como é que desinstalo o Bitdefender Password Manager?

Para desinstalar o Bitdefender Password Manager:

- No Windows e macOS:
  Remova a extensão do Password Manager do seu navegador. Clique com o botão direito do rato no ícone do Bitdefender e selecione “Remover”.
- Android:
  Toque e pressione a aplicação do Password Manager e, em seguida, arraste-a para o topo do ecrã onde diz “Desinstalar”.
- No iOS e iPadOS:
  Toque e prima a aplicação do Password Manager até que todas as aplicações no ecrã se comecem a mexer e, em seguida, toque no X no canto superior esquerdo do ícone do Bitdefender.

Perguntas de privacidade e segurança sobre o Bitdefender Password Manager

Os funcionários da Bitdefender podem ver minhas palavras-passe?

Não, de maneira alguma. A sua privacidade é a nossa maior prioridade. Esta é a principal razão pela qual não armazenamos a sua palavra-passe mestre nos nossos servidores de dados: para que ninguém tenha acesso à sua conta, nem mesmo os funcionários da empresa. Cada palavra-passe e conta são altamente encriptadas com o algoritmo de segurança de dados mais forte, e o código que vemos parece simplesmente uma sequência aleatória de números e letras misturadas.

O que aconteceria se os servidores do Password Manager fossem invadidos?

Cada palavra-passe está encriptada localmente no seu dispositivo antes de chegar perto dos nossos servidores, portanto, se hackers invadissem nosso sistema, eles só obteriam páginas de letras e números aleatórios sem a sua chave para as desencriptar. Isto significa que você e os dados das suas contas estão sempre seguros conosco.

7. CONSEGUINDO AJUDA

7.1. 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.

7.2. 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.

7.2.1. 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/.

7.2.2. 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/

7.2.3. 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/.

7.3. 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 31).

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

7.3.1. 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 uma chave exclusiva que pode ser comprada no varejo e usada 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 número de dispositivos e também pode ser usado para estender uma assinatura com a condição a 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 ligação direta temporária e encriptada para uma certa rede sobre uma rede menos segura. Desta forma, enviar e receber dados é seguro e encriptado, difícil de se tornar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com a utilização de um nome de utilizador e palavra-passe.

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.