GUIA DO UTILIZADOR

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Guia do usuário

Publication date 20/11/2024

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 SecurePass 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 SecurePass e o processo de instalação.

A importar e exportar as suas palavras-passe (página 10)

Entenda como você pode importar ou exportar senhas para dentro e para fora do SecurePass.

Características e Funcionalidades (página 14)

Aprenda a utilizar Bitdefender SecurePass e todas as suas funcionalidades.

Conseguindo ajuda (página 27)

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 SECUREPASS

Bitdefender SecurePass 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 SecurePass 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. 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 SecurePass em dispositivos que executem os seguintes sistemas operativos:

- **Para utilizadores de PC:**
  - Windows 7 com o Service Pack 1
  - 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 SecurePass 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 SecurePass ou na avaria do produto.

2.2. Instalação

Este capítulo irá guiá-lo sobre como instalar o Bitdefender SecurePass 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**.

- **Google Chrome**
- **Mozilla Firefox**

- **Microsoft Edge**
- **Safári**

Para instalar o Bitdefender SecurePass:

1. Depois de comprar o Bitdefender SecurePass, siga as etapas fornecidas no e-mail de confirmação para ativar sua assinatura.
2. Faça login no Bitdefender Central usando suas credenciais.
   No menu do lado esquerdo, selecione **Secure Pass**.
3. No painel SecurePass, selecione seu navegador preferido.
4. Instale a extensão do navegador:
   - **Google Chrome:**
     a. Clique no **Adicionar ao Chrome** botão.
     b. Na caixa de confirmação, clique em **Adicionar extensão**.
   - **Mozilla Firefox:**
     a. Clique no **Adicionar ao Firefox** botão.
     b. Clique no **Instalar** botão no canto superior direito da tela.
   - **Microsoft Edge:**
     a. Clique no **Obtenha** botão.
     b. Clique **Adicionar extensão** no prompt que aparece.
   - **Safári:**
     a. O instalador do SecurePass será baixado em seu dispositivo macOS. Clique duas vezes no arquivo baixado e siga as instruções na tela a partir daí
     b. Ao final do processo de instalação, abra o **Safári** navegador e selecione **Preferências** na barra de menu superior.
     c. Na janela Preferências, clique no **Aba Extensões**.
     d. Marque a caixa ao lado de **Bitdefender Secure Pass** para habilitá-lo.

Depois que a extensão estiver instalada, você poderá prosseguir para o Processo de configuração (página 8).

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.

1. Antes de mais nada, após a compra, certifique-se de abrir o e-mail de confirmação que você recebeu para seguir as instruções fornecidas para ativar sua assinatura do SecurePass.
2. Abra a Google Play Store em seu dispositivo Android.
3. Na barra de pesquisa da Google Play Store, digite **Bitdefender Secure Pass**, localize e baixe o aplicativo.
4. Quando o download estiver concluído, abra o aplicativo e, se necessário, siga as etapas de configuração na tela necessárias para concluir o processo de instalação.

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.

1. Antes de mais nada, após a compra, certifique-se de abrir o e-mail de confirmação que você recebeu para seguir as instruções fornecidas para ativar sua assinatura do SecurePass.
2. Abra a App Store em seu dispositivo iOS.
3. Na barra de pesquisa da App Store, digite **Bitdefender Secure Pass**, localize e baixe o aplicativo.
4. Quando o download estiver concluído, abra o aplicativo e, se necessário, siga as etapas de configuração na tela necessárias para concluir o processo de instalação.

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

2.3. Processo de configuração

Para configurar o Bitdefender SecurePass em seu navegador/dispositivo móvel:

1. Depois de concluir o processo de instalação, abra a extensão/aplicativo SecurePASS e faça o login.
   Use as credenciais da conta Bitdefender associada à sua assinatura do SecurePass.
2. Você será solicitado a criar um **Senha mestra**.

   Importante
   Observe que você precisará dessa senha mestra para desbloquear todas as senhas, informações de cartão de crédito e notas salvas no Bitdefender SecurePass. Essa é essencialmente a chave que permite ao proprietário usar esse produto.

   Certifique-se de inserir uma senha mestra forte sem correr o risco de esquecê-la facilmente.
   Depois de escolher uma senha mestra forte e exclusiva, clique em **Salvar e continuar**.
3. Em seguida, você receberá um **Chave de recuperação**.

   Aviso
   Ao criar a senha mestra, você receberá uma **Chave de recuperação de 24 dígitos**. Anote sua chave de recuperação em um local seguro e não a perca. Essa chave é a única maneira de acessar suas senhas salvas no Password Manager no caso de você **esqueça a senha mestra** configurado anteriormente para sua conta.

   - Salve a chave de recuperação copiando-a para a área de transferência ou baixando-a como um arquivo PDF.
     Você pode pressionar **Fechar** quando terminar.
4. Uma vez feito isso, selecione o **Acesse seu cofre** botão.

Agora que o processo de configuração foi concluído, você pode começar a usar o Bitdefender SecurePass.

3. 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.

3.1. Compatibilidade

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

- Gerenciador de senhas Bitdefender
- Carteira Bitdefender
- Bitdefender Secure Pass
- SaferPass
- 1 senha
- Kaspersky
- Dashlane
- Navegador Chrome
- Navegador Firefox
- Microsoft Edge
- Bitwarden
- LastPass
- Keepass
- RoboForm

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**.

3.2. 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. Abra o Bitdefender SecurePass e acesse **Configurações**.
   - No navegador:
     Clique em **Configurações** no canto superior direito da página.
   - No aplicativo:
     Toque no **Mais** botão no canto inferior direito da tela e, no topo da lista que aparece depois, toque em **Configurações**.
2. Na **Backup e restauração** seção, selecione **Importar senhas**. A janela de importação será aberta.
3. Selecione o nome do gerenciador de senhas ou do navegador da Web que você usou anteriormente no menu suspenso acessível por meio do **Selecione o tipo de arquivo** campo.

   > **Nota**
   > Se uma senha foi usada para criptografar o arquivo, você deverá inseri-la no **Senha** campo; caso contrário, você pode deixá-lo em branco.

4. Selecione o **Selecione o arquivo a ser importado** arquivado.
   Navegue até o local em que os dados exportados pertencentes ao seu antigo gerenciador de senhas foram salvos. Escolha o arquivo depois de encontrá-lo e clique em **Aberto**.

5. Depois de selecionar o arquivo, selecione **Importar** no canto inferior esquerdo da janela de importação. O processo começará em breve, acompanhado por uma barra de progresso.

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.

> **Nota**
> Voltando ao seu cofre de senhas no SecurePass, você notará uma pasta chamada **Importar**, contendo todos os dados do seu gerenciador de senhas ou navegador da web anterior.

3.3. 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. Abra o Bitdefender SecurePass e acesse **Configurações**.
   - No navegador:
     Clique em **Configurações** no canto superior direito da página.
   - No aplicativo:
     Toque no **Mais** botão no canto inferior direito da tela e, no topo da lista que aparece depois, toque em **Configurações**.
2. Na **Backup e restauração** seção, selecione **Exportar senhas**. A janela de exportação será aberta.

3. Clique em **Selecione o tipo de arquivo**. No menu suspenso, opte por exportar seus dados em formato JSON ou CSV. Você também pode inserir uma senha para proteger o arquivo exportado
   Marque a caixa correspondente se você também quiser incluir itens compartilhados.
4. Clique **Exportar** no canto inferior esquerdo da janela de exportação e salve o arquivo exportado no seu dispositivo.

4. 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.

4.1. Salvar senhas manualmente

Você pode armazenar com segurança informações como senhas, credenciais e outras, como informações de cartão de crédito ou notas no Bitdefender SecurePass manualmente, da seguinte maneira:

1. Abra o Bitdefender SecurePass
2. Na **Meu cofre** aba, pressione a tecla **+Adicionar item** botão.
3. Selecione o tipo de item que você deseja adicionar. (conta, cartão de crédito, identidade ou nota).
4. Preencha os campos obrigatórios dependendo do item selecionado.
5. Depois de preencher todos os detalhes necessários, salve o item para adicioná-lo ao seu cofre SecurePass.

4.2. Gerador de senhas

O Bitdefender SecurePass inclui um recurso de geração de senhas que pode ajudar na criação de senhas seguras.

Para acessar e usar o Gerador de Senhas:

1. Abra o Bitdefender SecurePass e acesse o **Gerar senha** aba no lado esquerdo da tela. Isso o levará ao Gerador de Senhas integrado ao SecurePass.
2. Personalize a senha que você está prestes a gerar de acordo com suas próprias necessidades e preferências.
   - Tamanho da senha: arraste o controle deslizante para determinar qualquer tamanho entre 8 e 32 caracteres.
   - Letras maiúsculas/minúsculas: selecione quais - ou ambos - tipos de letras você deseja adicionar para o nível de complexidade da sua senha.

- Números: Marcar essa caixa incluirá números na sequência de caracteres que compõe sua senha.
- Caracteres especiais: adicione símbolos à sua senha para aumentar a complexidade da senha.

> **Nota**
> Pressione o botão **Salvar configurações** botão para o SecurePass lembrá-los e sempre gerar senhas com base nas configurações que você salvou.

3. Gere uma nova senha clicando no ícone de seta circular localizado abaixo da senha exibida atualmente. Cada clique gera uma nova sequência de caracteres.
4. Quando estiver satisfeito com a senha gerada, você pode copiá-la para a área de transferência ou clicar no **Salvar conta** botão para armazená-lo em seu cofre (por associação com outras informações da conta).

> **Nota**
> Você também pode gerar rapidamente uma senha **diretamente dos formulários de inscrição** clicando no ícone Bitdefender SecurePass presente no campo de senha da página de inscrição. Clicando nele, você pode então escolher o **Gerar senha** opção.

4.3. Verificação da força da senha

O Bitdefender SecurePass oferece a possibilidade de avaliar a força das senhas salvas e dos dados confidenciais. Esse é um recurso vital na avaliação e avaliação de possíveis vulnerabilidades à privacidade e segurança de seus dados

Para verificar a força das senhas armazenadas:

1. Abra o Bitdefender SecurePass e, no menu de e-mail, selecione o **Relatório de segurança** aba.
   A guia Relatório de segurança está dividida em quatro seções: violada, fraca, antiga e duplicada.
2. O número de senhas que se enquadram em cada uma das quatro categorias será exibido na tela.

Além disso, examinando a lista de senhas armazenadas, cada senha será marcada com a categoria na qual está localizada.

Para entender o significado por trás desses níveis de segurança, abaixo estão alguns breves detalhes sobre cada um deles:

- Senhas violadas: se alguma de suas credenciais tiver sido parte de uma violação de dados, ela será listada na **violado** seção.

  > **Nota**
  > Para verificar se alguma de suas senhas foi comprometida e vazada por meio de violações de dados, clique no **Execute a verificação de segurança** botão.

- Senhas fracas: o SecurePass identificará e sinalizará **fraco** senhas armazenadas em seu cofre com base em um algoritmo interno executado localmente que analisa vários critérios, como tamanho da senha, variedade de caracteres e inclusão de dígitos ou letras maiúsculas, entre outros fatores.
- Senhas antigas: as senhas que foram salvas e não modificadas por um período superior a seis meses serão sinalizadas como **velho**.
- Senhas duplicadas: Considerando que usar as mesmas senhas em várias plataformas e contas representa um grande risco de segurança, o SecurePass sinalizará as senhas usadas em mais de um lugar como **duplicado**.

4.4. Organização de dados

No Bitdefender SecurePass, você pode organizar e, portanto, gerenciar com mais facilidade todos os seus itens salvos.

Você pode categorizar seus itens em pastas específicas para facilitar o acesso seguindo estas etapas:

1. Abra o Bitdefender SecurePass e acesse **Meu cofre**. Aqui, toque no **Adicionar pasta** botão.
2. Dê um nome à sua pasta e toque no **Criar** botão.
   A nova pasta agora aparecerá no seu cofre.

Para mover itens para a pasta criada:

1. Clique em qualquer conta que você deseja mover e pressione a tecla **Editar** botão.
2. Pressione a localização mostrada ao lado de **Salvar item em** e selecione o nome da pasta na lista suspensa.
3. Pressione o botão **Salvar conta** botão.

A conta agora será armazenada na pasta selecionada.

4.5. Preenchimento automático inteligente

O Bitdefender SecurePass permite que você preencha automaticamente as credenciais e informações da conta em qualquer formulário de login online.

> **Nota**
> Como uma extensão de navegador da web, no Windows ou no macOS, o recurso de preenchimento automático deve funcionar perfeitamente.

4.5.1. Preenchimento automático no Android

Para configurar o SecurePass no Android para usar o preenchimento automático:

1. Abra o aplicativo Bitdefender SecurePass em seu dispositivo Android.
2. Toque no **Mais** botão de menu.
3. Na parte superior da tela, toque em **Configurações**.
4. Toque em **Torne este seu gerenciador de senhas padrão**
5. Ative o Bitdefender SecurePass na lista de serviços de preenchimento automático.

> **Nota**
> Você também pode acessar as configurações do seu dispositivo Android, em **Senhas e contas** > **Serviço de preenchimento automático** > habilite o Bitdefender SecurePass.
>
> Para o Android 11 ou versões anteriores do sistema operacional, as configurações são: **Sistema** > **Idioma e entrada** > **Avançado**.

6. Toque **OK**.

Depois que essa configuração for concluída, sempre que você tocar em um campo de login, uma opção chamada Bitdefender SecurePass

aparecerá na sua tela. Você pode tocar nele para abrir o aplicativo. Faça login no SecurePass e suas credenciais serão preenchidas automaticamente

4.5.2. Preenchimento automático no iOS

Para configurar o SecurePass em seu dispositivo iOS para usar o preenchimento automático:

1. Abra o **Configuração** aplicativo no seu iPhone ou iPad e selecione **Geral**.
2. Toque em **Preenchimento automático e senhas**. Garanta a opção **Preenchimento automático de senhas e chaves de acesso** ou **Preenchimento automático de senhas** - dependendo da versão do iOS - está ativado.
3. Na **Formulário de preenchimento automático** lista, habilite o **Bitdefender Secure Pass** aplicativo.

Depois que essa configuração for concluída, sempre que você tocar em um campo de login, uma opção chamada Bitdefender SecurePass aparecerá na sua tela. Você pode tocar nele para abrir o aplicativo. Faça login no SecurePass e suas credenciais serão preenchidas automaticamente

4.5.3. Detalhes do cartão de preenchimento automático

Embora o SecurePass forneça um ícone de fácil acesso para preenchimento automático de credenciais e senhas de login, o recurso de preenchimento automático para informações de cartão de crédito funciona de forma diferente:

1. Navegue até a página de pagamento ou checkout do site no qual você deseja usar as informações armazenadas do cartão de crédito.
2. Clique com o botão direito do mouse em qualquer área em branco da página de pagamento. Isso fará com que o menu contextual apareça na tela
3. Selecione Bitdefender SecurePass no Menu passando o cursor sobre a opção. Isso abrirá um submenu com mais opções

4. Escolha o **Preencher automaticamente as informações do cartão de crédito**. Isso exibirá uma lista de todos os cartões de crédito que você armazenou no cofre do SecurePass
5. Selecione o cartão preferido.

Dessa forma, o SecurePass preencherá automaticamente os campos do formulário de pagamento com os detalhes do cartão de crédito que você escolheu.

5. USE COMO UM APLICATIVO 2FA

Você sempre pode optar por utilizar o Bitdefender SecurePass como um aplicativo autenticador de dois fatores para qualquer site ou plataforma que desejar e gerenciar seus códigos 2FA junto com suas senhas da seguinte maneira:

1. Acesse as configurações de segurança do site ou aplicativo em que você deseja ativar o recurso 2FA. Normalmente, você receberá um código QR ou um código de verificação durante o processo
2. Inicie o Bitdefender SecurePass e acesse a conta correspondente que você deseja configurar para uso 2FA. Clique no **Editar** botão.
3. Role até a parte inferior da página de entrada da conta no SecurePASS e pressione a tecla **Autenticação de dois fatores** opção.
4. Digitalize o código QR ou insira o código manualmente.
   Feito isso, o SecurePass confirmará a configuração bem-sucedida da autenticação de dois fatores.
5. Depois disso, pressione o novo **Exibir código** botão agora visível na interface. Um código sensível ao tempo é exibido lá
6. Volte para a conta em que você ativou o recurso 2FA e insira o código do Bitdefender SecurePass para verificar sua configuração.

Depois de concluir esse processo de configuração, pressione o botão **Salvar conta** botão no SecurePass para finalizar o processo.

A partir de agora, ao entrar na plataforma para a qual você configurou o recurso 2FA, você será solicitado a usar os códigos 2FA do SecurePass para a respectiva conta, oferecendo uma nova camada de segurança para a conta em questão.

6. COMPARTILHAR DADOS

O Bitdefender SecurePass vem com a possibilidade de compartilhar informações confidenciais com segurança, como credenciais, senhas ou detalhes do cartão de crédito.

Você pode usar o recurso de compartilhamento por meio de links:

1. Escolha um item armazenado em seu cofre.
   - No navegador:
     Vá até seu cofre e clique no item que você deseja compartilhar. No lado direito, clique no menu de três pontos e selecione **Compartilhar link**.
   - No aplicativo:
     Vá até o seu cofre e toque no item que você deseja compartilhar. Toque no ícone do link e escolha o **Gerar link de compartilhamento** opção.
2. Crie o link Compartilhar especificando:
   - A data de expiração do link.
   - O limite de uso.
   - Se o link deve ou não ser protegido por senha.
3. Depois de gerado, copie o link gerado e envie-o para o destinatário pretendido.

6.1. Compartilhe com grupos

Os grupos são criados com o objetivo de facilitar ainda mais o compartilhamento de dados. Você pode criar vários grupos dentro do Bitdefender SecurePass com outros usuários para compartilhar dados confidenciais com segurança

1. Crie um grupo:
   - Vá para **Grupos** e pressione a tecla **Criar grupo** botão na guia Grupos.
   - Defina um nome de grupo e pressione a tecla **Criar grupo** botão.

2. Adicionar itens aos grupos:
   - No navegador:
     Vá até seu cofre e clique no item que você deseja compartilhar. Clique no menu de três pontos no lado direito do item e escolha **Adicionar ao grupo**.
   - No aplicativo:
     Vá até seu cofre e clique no item que você deseja compartilhar. Escolha o **Compartilhe com o grupo** opção.

   Selecione o grupo com o qual você deseja compartilhar o item.
3. Defina os direitos de acesso (leitura, gravação, concessão) com base no nível de controle que você deseja fornecer aos membros do grupo.
4. Prensa **Salvar**, então **Feito**.

Você e os membros do grupo podem revisar os itens compartilhados na seção do grupo.

6.2. Gerenciar grupos

Na **Grupos** Na seção do Bitdefender SecurePass, você pode revisar todos os grupos criados e gerenciá-los com base em suas necessidades:

- Renomeie grupos.
- Edite membros. (convidar novos membros, atribuir direitos a membros específicos, conceder direitos de administrador ou de compartilhamento e remover membros existentes
- Saia dos grupos.
- Exclua grupos.

7. BLOQUEAR CONTA

O Bitdefender SecurePass vem com um **Bloquear conta** função que bloqueia instantaneamente sua conta e encerra todas as sessões ativas em todos os dispositivos que têm acesso a ela. Esse recurso é especialmente útil quando surgem suspeitas de acesso não autorizado

Para bloquear sua conta SecurePass:

1. Abra o Bitdefender SecurePass.
2. Uma vez no SecurePass:
   - No navegador:
     Clique em **Configurações** no canto superior direito da página.
   - No aplicativo móvel:
     Toque no **Proteja-me** botão de menu.
3. Pressione o botão **Bloquear conta** botão para sair instantaneamente de todos os dispositivos e encerrar as sessões em andamento.

8. 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

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 @).

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.

O que é o modo offline?

O modo offline é ativado automaticamente quando a conexão com a Internet cai ao usar o Bitdefender SecurePass. Se você já estiver conectado e tiver digitado sua senha mestra, o modo off-line permite acessar suas senhas quando uma conexão com a Internet estiver fora de alcance.

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.

9. CONSEGUINDO AJUDA

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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/

9.2.3. 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/.

9.3. 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 27).

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

9.3.1. 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.