GUIA DO UTILIZADOR

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security for iOS

Guia do usuário

Data de publicação 02/10/2023
Copyright © 2023 Bitdefender

Notícia legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou por qualquer sistema de armazenamento e recuperação de informações, sem permissão por escrito de um representante autorizado da Bitdefender. A inclusão de breves citações em resenhas pode ser possível apenas com a menção da fonte citada. O conteúdo não pode ser modificado de forma alguma.

Aviso e isenção de responsabilidade. Este produto e sua documentação são protegidos por direitos autorais. As informações neste documento são fornecidas "como estão", sem garantia. Embora todas as precauções tenham sido tomadas na preparação deste documento, os autores não terão qualquer responsabilidade perante qualquer pessoa ou entidade com relação a qualquer perda ou dano causado ou supostamente causado direta ou indiretamente pelas informações contidas neste trabalho.

Este livro contém links para sites de terceiros que não estão sob o controle da Bitdefender, portanto, a Bitdefender não é responsável pelo conteúdo de qualquer site vinculado. Se você acessar um site de terceiros listado neste documento, o fará por sua conta e risco. A Bitdefender fornece esses links apenas como uma conveniência, e a inclusão do link não implica que a Bitdefender endosse ou aceite qualquer responsabilidade pelo conteúdo do site de terceiros.

Marcas registradas. Nomes de marcas registradas podem aparecer neste livro. Todas as marcas comerciais registradas e não registradas neste documento são de propriedade exclusiva de seus respectivos proprietários e são reconhecidas com respeito.

Bitdefender

Índice

SOBRE ESTE GUIA

Propósito e público-alvo

Este guia é destinado a todos os utilizadores de iOS que escolheram o Bitdefender Mobile Security for iOS como solução de segurança para os seus dispositivos móveis. As informações apresentadas neste livro são apropriadas não só para aqueles com uma formação técnica, mas também para todas as pessoas capazes de trabalhar em dispositivos móveis Apple.

Descobrirá como configurar e utilizar o Bitdefender Mobile Security for iOS para se proteger contra ameaças e outras aplicações maliciosas. Aprenderá a aproveitar a Bitdefender ao máximo.

Desejamos-lhe uma leitura agradável e útil.

Como utilizar este guia

Este manual está organizado em diversos tópicos importantes:

Introdução (página 5)

Primeiros passos da Bitdefender Mobile Security for iOS e a sua interface de utilizador.

Características e Funcionalidades (página 9)

Saiba como utilizar o Bitdefender Mobile Security for iOS para se proteger contra ameaças e aplicações maliciosas, aprendendo sobre as suas características e funcionalidades.

Conseguindo ajuda (página 29)

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 O BITDEFENDER MOBILE SECURITY PARA IOS

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na Internet, fazem-se acompanhar de elevados riscos e, se os detalhes de segurança forem ignorados, os dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O Bitdefender Mobile Security para iOS permite que:

- Oferece a proteção mais poderosa contra as ameaças com o menor impacto sobre a bateria do dispositivo
- Proteja os seus dados pessoais: palavras-passe, endereço, informações sociais e financeiras
- Verifique facilmente a segurança do seu telemóvel para detetar e corrigir configurações erradas que a possam expor
- Evite a exposição acidental de dados e a utilização indevida para todas as aplicações instaladas
- Analise o seu dispositivo para obter definições de segurança e privacidade ideais
- Obtenha informações de utilização da sua atividade online e o histórico de incidentes prevenidos
- Verifique as suas contas online contra violações de dados ou fugas de dados
- Encripte o tráfego da internet com o VPN incluído

Bitdefender Mobile Security para iOS é entregue gratuitamente e requer ativação com uma conta **Bitdefender**. Contudo, algumas funcionalidades importantes da Bitdefender, tais como o nosso módulo "Proteção da Internet", requerem uma subscrição paga para que seja acessível aos nossos utilizadores.

2. INTRODUÇÃO

2.1. Requisitos do Aparelho

O Bitdefender Mobile Security para iOS funciona em qualquer dispositivo a executar o iOS 12 ou versões posteriores do sistema operativo e necessita de uma ligação ativa à Internet para ser ativado e para detetar se ocorreu alguma fuga de dados nas suas contas online.

2.2. Instalar o Bitdefender Mobile Security para iOS

- **Na Central Bitdefender**
  - Em iOS
    1. Aceda à **Central da Bitdefender**.
    2. Selecione o painel **Os Meus Dispositivos**.
    3. Toque em **INSTALAR PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Foi redirecionado para a aplicação da **App Store**. No ecrã da App Store, toque na opção de instalação.
  - No Windows, macOS e Android
    1. Acesso Bitdefender Central.
    2. Selecione os **Meus dispositivos** painel.
    3. Prima **INSTALAR PROTEÇÃO** e, em seguida, prima **Proteger outros dispositivos**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Prima **ENVIAR LIGAÇÃO DE TRANSFERÊNCIA**.
    6. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24

horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

7. No dispositivo em que deseja instalar o Bitdefender verifique a conta de e-mail que escreveu e pressione o botão de download correspondente.

- **Da App Store**
  Procure o Bitdefender Mobile Security para iOS e instale a aplicação.

É exibida uma janela introdutória com detalhes sobre as funções do produto na primeira vez que abrir a aplicação. Pressione Começar para avançar para o próximo passo.

Antes de passar pelos passos de validação, deve concordar com o Acordo de Subscrição. Leia o acordo de Subscrição com calma, já que ele contém os termos e condições segundo os quais pode utilizar o Bitdefender Mobile Security for iOS.

Toque em **Continuar** para avançar para a janela seguinte.

2.3. Entre na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security for iOS, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google, Apple ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Para vincular o seu dispositivo a uma conta Bitdefender:

1. Introduza o seu endereço de e-mail da sua conta da Bitdefender no respetivo campo e clique em **PRÓXIMO**. Se não tem uma conta da Bitdefender e pretende criar uma, selecione a respetiva hiperligação e depois siga as instruções no ecrã até a conta ser ativada.
   Para entrar usando uma conta do Facebook, Google, Apple ou Microsoft, pressione o serviço que deseja usar na área **Ou entrar com**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security for iOS.

Observação

O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

2. Introduza a sua palavra-passe e depois toque em **ENTRAR**.

A partir daqui pode também aceder à Política de Privacidade da Bitdefender.

2.4. Painel de instrumentos

Toque no ícone do Bitdefender Mobile Security for iOS nas aplicações do seu dispositivo para abrir a interface da aplicação.

Na primeira vez que abrir a aplicação, será solicitado a permitir ao Bitdefender o envio de notificações. Prima **Permitir** para permanecer informado sempre que o Bitdefender tiver de comunicar algo relevante para a sua aplicação. Para gerir as notificações do Bitdefender, aceda a Definições > Notificações > Segurança móvel.

Para ter acesso à secção de que necessita, toque no ícone correspondente a partir da parte inferior do ecrã.

Proteção da Internet

Fique seguro(a) enquanto navega na Internet e quando aplicações menos seguras tentarem aceder a domínios não fiáveis. Para obter mais informações, aceda a Proteção da Internet (página 11).

VPN

Mantenha a sua privacidade independentemente da rede à qual estiver ligado(a) para manter a sua comunicação pela Internet encriptada. Para mais informações, aceda a VPN (página 13).

Privacidade de Conta

Saiba se as suas contas de e-mail foram invadidas ou não. Para mais informação, dirija-se a Privacidade da conta (página 16).

Para ver mais opções, toque no ícone ••• no dispositivo enquanto estiver no ecrã inicial da aplicação. São apresentadas as seguintes opções:

- **Restaurar compras** - aqui pode restaurar as antigas subscrições que comprou através da conta do iTunes.

- **Definições** - aqui tem acesso a:
  - **Definições de VPN**
    - **Contrato** - pode ler os termos de utilização do serviço VPN de Bitdefender. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.
    - **Abrir aviso de Wi-Fi** - pode ativar ou desativar a notificação do produto que é apresentada sempre que estabelecer ligação a uma rede Wi-Fi não segura.
      O objetivo desta notificação é ajudá-lo a manter os seus dados privados e seguros utilizando a VPN de Bitdefender.
  - **Definições de proteção da Internet**
    - **Contrato** - pode ler os termos de utilização da Proteção Bitdefender na Web. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.
    - **Ativar notificações da Proteção na Web** - Será notificado(a) para lembrar que a Proteção na Web pode ser ativada após o fim de uma sessão VPN.
  - **Relatórios do produto**
- **Comentários** — aqui pode iniciar o cliente de e-mail predefinido para nos enviar comentários sobre a aplicação.
- **Informações sobre a aplicação** — aqui tem acesso a informações sobre a versão instalada e o Contrato de Subscrição, Política de Privacidade e conformidade com licenças de código aberto.

3. CARACTERÍSTICAS E FUNCIONALIDADES

3.1. Análise

O Bitdefender Mobile Security para iOS permite-lhe verificar no seu dispositivo quaisquer vulnerabilidades de segurança e potenciais ameaças no seu dispositivo. A realização da análise irá verificar a existência de:

- **Versão do SO:** a verificar as atualizações mais recentes da sua versão iOS.
- **Código de acesso/Biometria:** verificar o nível de segurança em relação ao acesso ao seu dispositivo.
- **Proteção da Internet:** verificar o estado do módulo de Proteção da Internet
- **Privacidade da conta:** verificar a presença de contas monitorizadas listadas no módulo Privacidade da conta.
- **Analisar Wi-Fi:** verificar o estado de segurança da rede atualmente ligada.

O estado de proteção é determinado depois de executar uma análise manual.

Depois de executar a primeira análise, verá as **Recomendações do Autopilot** da Bitdefender. Este é o seu conselheiro de segurança pessoal, que lhe fornece recomendações contextuais com base na utilização e necessidades do seu dispositivo. Desta forma, poderá beneficiar de tudo o que a sua aplicação tem para oferecer.

> **Observação**
> Ao entrar na aplicação pela primeira vez, ser-lhe-á pedido que realize uma análise.

3.2. Alerta de fraude

O recurso Alerta de Golpe disponível no Bitdefender Mobile Security para iOS protege proativamente os usuários da Apple contra golpes de phishing. O Scam Alert para iOS inclui duas camadas de proteção que monitoram golpes entregues por meio de mensagens SMS/MMS e convites de calendário:

- **Filtro de mensagens de texto (SMS, MMS)**
  Este recurso identifica e filtra mensagens SMS e MMS indesejadas.
  Um SMS/MMS (serviço de mensagens curtas/serviço de mensagens multimídia) malicioso refere-se a um tipo de mensagem enviada a dispositivos móveis com intenções prejudiciais. Essas mensagens são projetadas para explorar vulnerabilidades, enganar destinatários ou causar danos ao dispositivo, às informações pessoais ou à segurança do alvo.
- **Scanner de link de convite de calendário**
  Este recurso detecta calendários de spam e eventos que contêm links perigosos. O vírus de calendário é um tipo de spam que afeta o aplicativo Calendário do seu iPhone, o que pode ser irritante e potencialmente perigoso:
  - Você recebe convites de calendário ou notificações de eventos indesejados quando aceita acidentalmente um convite de calendário falso enviado para seu endereço de e-mail por hackers ou spammers.
  - Ao clicar no link do convite, você inadvertidamente se inscreve no calendário do remetente, o que permite que ele envie mais eventos de spam.
  - Os eventos de spam podem conter links ou anexos que podem levar você a páginas de phishing ou outras ameaças cibernéticas, caso você os abra.

3.2.1. Como configurar o Alerta de Golpe

Para ativar o Alerta de Fraude, você precisa conceder ao aplicativo Bitdefender Mobile Security acesso a notificações de calendário e mensagens SMS:

Como ativar a filtragem de SMS:

Para que o Bitdefender comece a filtrar mensagens, você deve ativar manualmente a opção Filtrar Remetentes Desconhecidos nas configurações do aplicativo Mensagens:

1. Abra o **Configurações** aplicativo no seu iPhone ou iPad.
2. Role para baixo e selecione **Mensagens** na lista.
3. Toque em **Desconhecido e spam** seção.

4. Alternar **Filtrar remetentes desconhecidos** para a posição ligado.
5. Selecione **Segurança para celulares** na seção Filtragem de SMS e escolha **Habilitar**.

O Bitdefender agora será capaz de filtrar mensagens indesejadas no seu iPhone/iPad.

> **Observação**
> Devido às restrições do iOS, a filtragem de SMS do Bitdefender só pode ser usada para mensagens SMS e MMS provenientes de pessoas que você não salvou em seus contatos. Isso significa que ele não filtrará mensagens de pessoas que já estão na sua lista de contatos ou mensagens do iMessage de ninguém.

Como ativar a verificação de calendário:

1. Abra o **Segurança Móvel Bitdefender** aplicativo instalado no seu iPhone ou iPad.
2. Vou ao **Alerta de fraude** opção na barra de navegação inferior e pressione **Configurar agora**.
3. Tocar **Continuar** e toque em **Habilitar**.
4. Escolher **OK** para conceder ao Bitdefender acesso ao seu calendário. Uma verificação do calendário começará imediatamente.

3.3. Proteção da Internet

A Proteção da Web do Bitdefender garante uma experiência de navegação segura alertando-o sobre páginas da Internet maliciosas e quando aplicações instaladas menos seguras tentam aceder a domínios não fiáveis.

Quando um URL sinalizar uma página da Internet conhecida como phishing ou fraudulenta, ou como tendo conteúdo malicioso como spyware ou vírus, a página da Internet é bloqueada e é exibido um alerta. Acontece a mesma coisa quando aplicações instaladas tentam aceder a domínios maliciosos.

> **Importante**
> Se está numa área onde a utilização de um serviço VPN é limitado por lei, a função de Proteção na Internet não estará disponível.

Para ativar a Proteção na Internet:

1. Toque no ícone na parte inferior do ecrã.
2. Toque em **Concordo**.
3. Ativar a chave de Proteção na Internet.

> **Observação**
> A primeira vez que ligar a Proteção na Internet, deverá permitir ao Bitdefender definir as configuração de VPN que irão monitorizar o tráfego de rede. Pressione **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de impressão digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize. Para poder detetar o acesso a domínios não fiáveis, a Proteção na Internet trabalha em conjunto com os serviços VPN.

> **Importante**
> A funcionalidade de Proteção na Web e o VPN não podem funcionar ao mesmo tempo. Sempre que um deles for ativado, o outro (caso esteja ativo nessa altura) será desativado.

3.3.1. Alertas Bitdefender

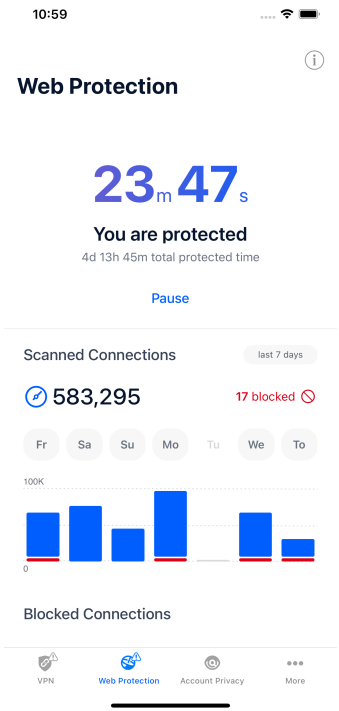
Sempre que tentar visitar um site classificado como não seguro, será bloqueado. Para avisá-lo sobre o evento, será notificado pelo Bitdefender no centro de Notificações e no seu navegador. A página de alertas contém informações como o URL do site e a ameaça detetada. Tem de decidir o que fazer a seguir.

Além disso, receberá notificações no Centro de Notificações quando uma aplicação menos segura tentar aceder a domínios não fiáveis. Clique na notificação exibida para ser redirecionado(a) para a janela onde poderá decidir o que fazer a seguir.

As seguintes opções estão disponíveis para os dois casos:

- Sair do site tocando em **VOLTAR À SEGURANÇA**.
- Ir para o site apesar do aviso tocando na notificação mostrada e, em seguida, em **Quero aceder à página**.

Confirme a sua escolha.



3.4. VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual está ligado, protegendo a sua ligação, encriptando os seus dados com encriptação de nível militar e ocultando o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado através de um servidor separado, fazendo com que o seu dispositivo seja impossível de identificar pelo seu ISP, entre os incontáveis dispositivos que utilizam os nossos serviços. Além disso, enquanto estiver ligado à internet através do Bitdefender Mobile Security for iOS, poderá aceder a conteúdos que normalmente são restritos em áreas específicas.

> **Observação**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação Bitdefender VPN pela primeira vez. Ao continuar a utilizar a aplicação, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

Para ativar o Bitdefender VPN:

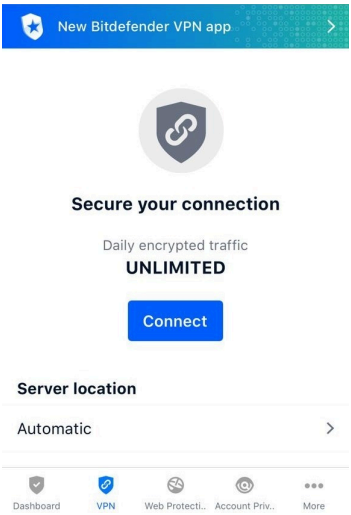
1. Toque em ícone na parte inferior da tela.
2. Pressione **Ligarr** sempre que quiser permanecer protegido enquanto estiver ligado às redes sem fios não seguras.
   Pressione **Desconectar** quando desejar desativar a ligação.

> **Observação**
> Na primeira vez que ligar o VPN, será solicitado a permitir que o Bitdefender faça configurações de VPN que monitorizarão o tráfego de rede. Prima **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize.

O ícone do VPN aparece na barra de estado quando a VPN está ativa.

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Se tiver uma subscrição Premium e quiser ligar-se a um servidor da sua escolha, pressione Automático na interface de VPN e, em seguida, selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a Subscrições (página 15).



3.4.1. Subscrições

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar e liga-o automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar a versão do Bitdefender VPN Premium a qualquer momento tocando no botão **Ativar VPN Premium** disponível na janela do VPN. Existem dois tipos de subscrição disponíveis: anual e mensal.

A subscrição Bitdefender Premium VPN é independente da subscrição grátis do Bitdefender Mobile Security for iOS, ou seja, poderá usá-lo por todo o seu período de disponibilidade. Caso a subscrição Bitdefender Premium VPN expire, voltará automaticamente para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Ao atualizar para o plano premium, pode utilizar a sua subscrição em todos os produtos, desde que inicie sessão com a mesma conta da Bitdefender.

Observação

O Bitdefender VPN também funciona como uma aplicação autónoma em todos os sistemas operativos suportados, incluindo Windows, macOS, Android e iOS.

3.5. Privacidade da conta

A Privacidade de Conta do Bitdefender deteta se ocorreu qualquer fuga de dados nas contas que utiliza para fazer pagamentos, compras ou subscrições online em diferentes aplicações e websites. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

Para verificar se qualquer conta foi invadida, toque em **Procurar fugas**.

Para começar a proteger informações pessoais:

1. Toque em ícone na parte inferior da tela.
2. Toque em **Adicionar conta**.
3. Digite o seu endereço de e-mail no campo correspondente e toque em **Seguinte**.
   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.
4. Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.
   O estado de privacidade da conta validada é apresentado.

Se forem detetadas fugas nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) fuga(s) identificada(s) como **Resolvido**. Para tal:

1. Toque em ··· ao lado da infração que resolveu.
2. Toque em **Marcar como resolvido**.

Quando todas as fugas detetadas estiverem marcadas como Resolvido, a conta já não aparece como fuga, pelo menos até à deteção de uma nova fuga.

4. SOBRE A CENTRAL BITDEFENDER

A Central Bitdefender é a plataforma onde tem acesso aos recursos e serviços online do produto e pode realizar remotamente tarefas importantes em dispositivos nos quais o Bitdefender estiver instalado. Você pode entrar na sua conta da Bitdefender a partir de qualquer computador ou telemóvel ligado à internet ao aceder ao https://central.bitdefender.com, ou diretamente da aplicação da Central Bitdefender em dispositivos Android e iOS.

Para instalar a aplicação da Central Bitdefender nos seus dispositivos:

- **Em Android** - procure por Bitdefender Central no Google Play e descarregue e instale a aplicação. Siga os passos necessários para completar a instalação.
- **Em iOS** - procure por Bitdefender Central na App Store e descarregue e instale a aplicação. Siga os passos necessários para completar a instalação.

Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para transferência são:
  - Bitdefender Mobile Security para iOS
  - Bitdefender Mobile Security for Android
  - Bitdefender Antivirus for Mac
  - A linha de produtos da Bitdefender para Windows
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

4.1. Aceda à Central Bitdefender

Existem duas maneiras de aceder à Central Bitdefender

- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.
  2. Vá a: https://central.bitdefender.com.

3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.

❍ No seu dispositivo Android ou iOS:
Abra a aplicação da Central Bitdefender que instalou.

> **Observação**
> Neste material incluímos as opções que pode encontrar na interface na web.

4.2. Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao solicitar um código de autenticação além das credenciais de início de sessão. Assim, irá impedir o roubo da conta e irá prevenir diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

4.2.1. Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, irá deixar a sua conta Bitdefender muito mais segura. A sua identidade será verificada sempre que iniciar sessão num dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Acesso Bitdefender Central.
2. Clique no ícone no lado superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu suspenso.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **COMEÇAR**.
Selecione uma das seguintes opções:

❍ **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.
Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

a. Clique em **UTILIZAR APLICAÇÃO DE AUTENTICAÇÃO** para começar.

b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.
Para iniciar sessão utilizando um portátil ou um computador, pode adicionar manualmente o código apresentado.
Clique em **CONTINUAR**.

c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, clique em **ATIVAR**.

- **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique o seu email e utilize o código que lhe foi enviado.

  a. Clique em **UTILIZAR E-MAIL** para começar.

  b. Verifique a sua conta de e-mail e introduza o código fornecido.
  Lembre que tem cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

  c. Clique em **ATIVAR**.

  d. Receberá dez códigos de ativação. Pode copiar, transferir ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário não poderá iniciar sessão. Cada código pode ser utilizado apenas uma vez.

  e. Toque em **PRONTO**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.
   Caso tenha escolhido receber o código de autenticação por e-mail, terá cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.
3. Confirme sua escolha.

4.3. Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Acesso Bitdefender Central.
2. Toque em ícone no canto superior direito da tela.
3. Tocar **Conta Bitdefender** no menu de slides.
4. Selecione os **Senha e segurança** aba.
5. Clique em **Dispositivos de confiança**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

4.4. Meus dispositivos

A secção **Os Meus Dispositivos** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

4.4.1. Adicione um novo dispositivo

Caso a sua subscrição cubra mais do que um dispositivo, pode adicionar um novo dispositivo e instalar o seu Bitdefender Mobile Security for iOS no mesmo, conforme descrito abaixo:

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel e, em seguida, toque em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**

Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, toque no botão correspondente.

- **Proteger outros dispositivos**
  Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, toque no botão correspondente.
  Clique em **ENVIAR LINK PARA A TRANSFERÊNCIA**. Introduza um endereço de e-mail no campo correspondente, e clique em **ENVIAR E-MAIL**. Saiba que o link gerado para a transferência é válido apenas durante as próximas 24 horas. Se o link expirar, deve gerar um link novo ao seguir os mesmos passos.
  No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e toque no botão de download correspondente.

4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

4.4.2. Personalize o seu dispositivo

Para identificar facilmente os seus dispositivos, pode personalizar o nome de cada um:

1. Acesso Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Configurações**.
5. Introduza um nome novo no campo **Nome do dispositivo**, depois clique em **GUARDAR**.

Pode criar e atribuir um proprietário a cada um dos seus dispositivos para uma melhor gestão:

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel.

3. Toque no cartão do dispositivo desejado e, em seguida, no ⋮ ícone no canto superior direito da tela.
4. Selecione **Perfil**.
5. Clique em **Adicionar proprietário** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento, além de um e-mail e número de telefone.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

4.4.3. Ações remotas

Para atualizar o Bitdefender remotamente no dispositivo:

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel.
3. Toque no cartão do dispositivo desejado e, em seguida, no ⋮ ícone no canto superior direito da tela.
4. Selecione **Atualizar**.

Para mais ações remotas e informações sobre o seu produto Bitdefender num dispositivo específico, clique no cartão de dispositivo pretendido.

Quando clicar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel.** Nesta janela, pode ver detalhes sobre o dispositivo selecionado, verifique o seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas afetando seu dispositivo, amarelo, quando o dispositivo solicitar a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique na seta suspensa na área de estado superior para saber mais detalhes. Aqui,
- **Proteção.** Nesta janela, pode executar uma Verificação do Sistema ou uma Verificação Rápida dos seus dispositivos remotamente. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir

quando a última verificação foi realizada no dispositivo e aceder um relatório da última verificação, contém as informações mais importantes.

- **Otimizador.** Aqui pode melhorar remotamente o desempenho de um dispositivo através da digitalização rápida, deteção e limpeza de ficheiros inúteis. Clique no botão **INICIAR** e, em seguida, selecione as áreas que deseja otimizar. Clique novamente no botão **INICIAR** para iniciar o processo de otimização. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre as questões corrigidas.
- **Antifurto.** Em caso de extravio, furto ou perda, com a funcionalidade Antifurto, pode localizar o seu dispositivo e tomar ações remotas. Clique em **LOCALIZAR** para descobrir a localização do dispositivo. A última localização conhecida será exibida, com a hora e a data.
- **Vulnerabilidade.** Para verificar um dispositivo em pesquisa de qualquer vulnerabilidade, como atualizações do Windows ausentes, aplicações desatualizadas ou palavras-passe fracas, clique no botão **VERIFICAR** no separador Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente. Caso qualquer vulnerabilidade seja descoberta, é necessário executar uma verificação nova no dispositivo e, em seguida, tomar as ações recomendadas. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre os problemas encontrados.

4.5. Actividade

Na área de Atividades, tem acesso à informação sobre os dispositivos que têm o Bitdefender instalado.

Ao aceder a janela **Atividade**, os seguintes cartões são disponibilizados:

- **Meus dispositivos.** Aqui pode ver o número dos dispositivos ligados juntamente com seu estado de proteção. Para corrigir problemas remotamente nos dispositivos detetados, clique em **Corrigir problemas**, e depois, clique em **VERIFICAR E RESOLVER OS PROBLEMAS**.

  Para visualizar detalhes sobre os problemas detectados, clique em **Visualizar problemas**.

  Informações sobre ameaças detectadas não podem ser recuperadas de dispositivos iOS.

- **Ameaças bloqueadas.** Aqui pode visualizar um gráfico que mostra uma estatística geral que inclui informação sobre as ameaças bloqueadas nas últimas 24 horas e nos últimos sete dias. A informação exibida vai depender do comportamento malicioso detectado e os ficheiros, aplicações e URLs acedidos.
- **Utilizadores principais com ameaças bloqueadas.** Aqui pode visualizar uma lista que mostra onde o maior número ameaças para os utilizadores foram identificadas.
- **Dispositivos principais com ameaças bloqueadas.** Aqui pode visualizar uma lista mostrando onde foram encontrados os dispositivos com o maior número de ameaças.

4.6. As minhas subscrições

A plataforma da Bitdefender Central possibilita-lhe controlar facilmente as subscrições que possui para todos os seus dispositivos.

4.6.1. Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Acesso Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.

Aqui pode aceder às informações sobre a disponibilidade das subscrições que possui e o número de dispositivos a utilizar cada uma delas.

Pode adicionar um novo dispositivo a uma subscrição ou renová-la selecionando um cartão de subscrição.

> **Observação**
> Pode ter uma ou mais subscrições na sua conta desde que sejam para diferentes plataformas (Windows, macOS, iOS ou Android).

4.6.2. Ativar subscrição

É possível ativar uma subscrição durante o processo de instalação ao utilizar a sua conta Bitdefender. Juntamente com o processo de ativação, a validade da subscrição inicia a sua contagem decrescente.

Se tiver comprado um código de ativação de um dos nossos revendedores ou o tiver recebido como presente, pode adicionar a sua disponibilidade à sua subscrição do Bitdefender.

Para ativar uma subscrição com um código de ativação, siga os passos abaixo:

1. Acesso Bitdefender Central.
2. Selecione os **Minhas assinaturas** painel.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A subscrição está ativada agora.

4.6.3. Renovar subscrição

Caso tenha desativado a renovação automática da sua subscrição do Bitdefender, pode renová-la manualmente seguindo estas instruções:

1. Acesso Bitdefender Central.
2. Selecione os **Minhas assinaturas** painel.
3. Selecione o cartão de subscrição pretendido.
4. Clique em **RENOVAR** para continuar.

Uma página abrirá no seu navegador onde poderá renovar a sua subscrição do Bitdefender.

4.7. Notificações

Para o ajudar a manter-se informado sobre o que se passa com os dispositivos associados à sua conta, o ícone é útil. Quando clicar sobre este ícone, terá uma imagem global que é composta pelas informações sobre a atividade dos produtos do Bitdefender instalados nos seus dispositivos.

5. PERGUNTAS FREQUENTES

Como é que o Bitdefender Mobile Security for iOS me protege contra vírus, malware e ciberameaças?

O Bitdefender Mobile Security for iOS fornece proteção absoluta contra todas as ciberameaças e está especialmente concebido para manter os seus dados sensíveis protegidos contra olhares curiosos.

Obtém uma ampla variedade de funcionalidades de segurança e privacidade para o seu iPhone e iPad - além de muitas funcionalidades de bónus, incluindo o VPN e a Proteção na Web.

O Bitdefender Mobile Security for iOS reage instantaneamente ao vírus e malware sem comprometer o desempenho do seu sistema.

Que tipo de dispositivos e sistemas operativos são abrangidos pelo Bitdefender Mobile Security for iOS?

O Bitdefender Mobile Security for iOS protegerá os seus smartphones e tablets com iOS contra todas as ciberameaças.

Por que é que eu preciso do Bitdefender Mobile Security for iOS no sistema operativo da Apple?

Alguns dos seus dados mais pessoais estão armazenados no seu iPhone ou iPad - e precisa de saber se eles estão seguros a qualquer momento. O Bitdefender Mobile Security for iOS oferece proteção absoluta e informações privadas sem interferência nas suas atividades diárias.

Recebo uma VPN juntamente com a minha subscrição do Bitdefender Mobile Security for iOS?

O Bitdefender Mobile Security para iOS inclui uma versão básica do Bitdefender VPN que inclui uma quantidade generosa de tráfego (200 MB/dia, um total de 6 GB/mês) gratuitamente.

6. CONSEGUINDO AJUDA

6.1. 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.

6.2. 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.

6.2.1. 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/.

6.2.2. 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/

6.2.3. 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/.

6.3. 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 29).

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

6.3.1. 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.