Bitdefender®
MOBILE SECURITY

GUIA DO UTILIZADOR

Bitdefender Mobile Security

Guia do usuário

Data de publicação 22/11/2022

Notícia legal

Bitdefender

Índice

Sobre este guia **1**
Propósito e público-alvo 1
Como utilizar este guia 1
Convenções utilizadas neste guia 1
Convenções Tipográficas 1
Avisos 2
Pedido de Comentários 2
1. O que é o Bitdefender Mobile Security **4**
2. Introdução **5**
2.1. Requisitos do Aparelho 5
2.2. Instalar o Bitdefender Mobile Security 5
2.3. Entre na sua conta Bitdefender 6
2.4. Configurar proteção 7
2.5. Painel 8
3. Características e Funcionalidades **11**
3.1. Analisador de Malware 11
3.2. Proteção da Internet 13
3.3. VPN 14
3.3.1. Definições da VPN 16
3.3.2. Assinaturas 17
3.4. Scam Alert 17
3.4.1. Ativar o Scam Alert 18
3.4.2. Proteção de chat em tempo real 19
3.5. Funcionalidades Anti Furto 20
3.5.1. A ativar o Anti Furto 21
3.5.2. Usar as funcionalidades Anti-Roubo a partir da Bitdefender Central 22
3.5.3. Funcionalidades Antirroubo 23
3.6. Privacidade de conta 23
3.7. Bloqueio de Aplicativo 25
3.7.1. A ativar o Bloqueio de Aplicação 25
3.7.2. MODO DE BLOQUEIO 27
3.7.3. Definições do Bloqueio de Aplicação 27
3.7.4. Tirar foto 28
3.7.5. Desbloqueio Inteligente 29
3.8. Relatórios 29
3.9. WearON 30
3.9.1. A ativar o WearON 31
3.10. Sobre 31

4. Sobre a Central Bitdefender 32
4.1. Aceda à Central Bitdefender 32
4.2. Autenticação de dois fatores 33
4.2.1. Ativar autenticação de dois fatores 33
4.3. Adicionar dispositivos fiáveis 35
4.4. Meus dispositivos 35
4.4.1. Adicione um novo dispositivo 35
4.4.2. Personalize o seu dispositivo 36
4.4.3. Ações remotas 37
4.5. Actividade 38
4.6. As minhas subscrições 39
4.6.1. Verificar subscrições disponíveis 39
4.6.2. Ativar subscrição 39
4.6.3. Renovar subscrição 40
4.7. Notificações 41
5. Perguntas Frequentes 42
6. Conseguindo ajuda 48
6.1. Pedir Ajuda 48
6.2. Recursos Em Linha 48
6.2.1. Centro de Suporte da Bitdefender 48
6.2.2. A Comunidade de Especialistas da Bitdefender 49
6.2.3. Bitdefender Cyberpedia 49
6.3. Informações de Contato 50
6.3.1. Distribuidores locais 50
Glossário 51

SOBRE ESTE GUIA

Propósito e público-alvo

Este guia é destinado a todos os utilizadores de Android que escolheram o Bitdefender Mobile Security 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 Android.

Descobrirá como configurar e utilizar o Bitdefender Mobile Security 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 e a sua interface de utilizador.

Características e Funcionalidades (página 11)

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

Conseguindo ajuda (página 48)

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

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** permite-lhe:

- Obtenha a melhor proteção para o seu smartphone e tablet Android com impacto mínimo na duração da bateria
- Proteja-se contra a ameaça de virar vítima de fraudes com base em ligações
- Ganhe acesso ao nosso VPN seguro para uma experiência rápida, anónima e segura enquanto navega na internet
- Localize, bloqueie e limpe o seu dispositivo Android remotamente em caso de perda ou furto
- Verifique se a sua conta de e-mail esteve envolvida em vazamentos ou violações de dados

2. INTRODUÇÃO

2.1. Requisitos do Aparelho

O Bitdefender Mobile Security funciona em qualquer dispositivo que execute o Android 5.0 ou em qualquer versão posterior do sistema operativo. É necessária uma ligação ativa à internet para a verificação de ameaças na nuvem.

2.2. Instalar o Bitdefender Mobile Security

- **Na Central Bitdefender**
  - Android
    1. Vá a: https://central.bitdefender.com.
    2. Entre na sua conta Bitdefender.
    3. Selecione o painel **Os Meus Dispositivos**.
    4. Toque em **INSTALAR PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
    5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    6. Você será redirecionado para a aplicação do **Google Play**. No ecrã do Google Play, pressione a opção de instalação.
  - No Windows, macOS e iOS
    1. Vá para: https://central.bitdefender.com.
    2. Entre na sua conta Bitdefender.
    3. Selecione os **Meus dispositivos** painel.
    4. Prima **INSTALAR PROTEÇÃO** e, em seguida, prima **Proteger outros dispositivos**.
    5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    6. Prima **ENVIAR LIGAÇÃO DE TRANSFERÊNCIA**.
    7. 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.

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

- **No Google Play**
  Procure o Bitdefender Mobile Security para localizar e instalar a aplicação.
  Alternativamente, analise o código QR:

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

2.3. Entre na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security, 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.

Se instalou o Bitdefender Mobile Security a partir da sua conta Bitdefender, a aplicação tentará entrar automaticamente nessa conta.

Para vincular o seu dispositivo a uma conta Bitdefender:

1. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.

2. Toque em **INICIAR SESSÃO**.

Para entrar usando uma conta do Facebook, Google 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.

> **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.

2.4. Configurar proteção

Uma vez que consiga entrar na aplicação, a janela Configurar proteção aparecerá. Nós recomendamos que realize estes passos para proteger o seu dispositivo:

- **Estado de subscrição**. Para obter a proteção do Bitdefender Mobile Security, deve ativar o seu produto com uma subscrição, que especificará por quanto tempo poderá utilizar o produto. Assim que esse período acabar, a aplicação irá parar de realizar as suas funções e de proteger o seu dispositivo.
  Se tiver um código de ativação, toque em **TENHO UM CÓDIGO**, e depois toque em **ATIVAR**.
  Se tiver entrado com uma nova conta Bitdefender e não tiver um código de ativação, poderá utilizar o produto por 14 dias gratuitamente.
- **Proteção na Web**. Se o seu dispositivo requer Acessibilidade para ativar a Proteção na Web, toque em **ATIVAR**. Será redirecionado para o menu de Acessibilidade. Toque em Bitdefender Mobile Security e depois ative o botão correspondente.
- **Analisador de malware**. Realize uma análise única do seu dispositivo para se certificar que ele esteja livre de ameaças. Para iniciar o processo de análise, toque em **ANALISAR AGORA**.
  Assim que o processo de análise começar, o painel aparecerá. Aqui vê o estado de segurança do seu dispositivo.

2.5. Painel

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

O Painel fornece informações sobre o estado de segurança do seu dispositivo e através do Autopilot, ele ajuda a reforçar a segurança do seu dispositivo oferecendo recomendações de funcionalidades.

O cartão de estado no topo da janela informa sobre o estado de segurança do dispositivo utilizando mensagens explícitas e cores sugestivas. Se o Bitdefender Mobile Security não tiver alertas, o cartão de estado será verde. Quando um problema de segurança é detectado, a cor do cartão de estado muda para vermelho.

Para oferecer uma operação eficaz e uma proteção aprimorada enquanto realiza diferentes atividades, o **Bitdefender Autopilot** atuará como seu consultor pessoal de segurança. Dependendo da atividade que você realizar, o Bitdefender Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. Isso irá ajudá-lo a descobrir e se beneficiar das vantagens trazidas pelos recursos incluídos na aplicação do Bitdefender Mobile Security.

Quando houver um processo em curso ou uma função solicitar uma ação sua, é exibido um cartão com mais informações e ações possíveis no Painel de Controlo.

É possível aceder às funcionalidades de Bitdefender Mobile Security e navegar facilmente da barra de navegação inferior:

Analisador de malware

Permite que inicie uma análise sob demanda e que ative o Armazenamento da Análise. Para mais informação, dirija-se a Analisador de Malware (página 11).

Proteção da Internet

Garante uma experiência de navegação segura alertando-lhe sobre páginas Web potencialmente maliciosas. Para mais informação, dirija-se a Proteção da Internet (página 13).

VPN

Encripta a comunicação na Internet, ajudando-o a manter a sua privacidade, não importando a rede à qual está ligado. Para mais informação, dirija-se a VPN (página 14).

Scam Alert

Garante a sua segurança ao alertá-lo sobre hiperligações maliciosas que chegam via SMS, aplicações de mensagens e qualquer tipo de notificação. Para mais informações, consulte Scam Alert (página 17).

Antifurto

Permite que ative ou desative as características Anti Furto e configure as definições Anti Furto. Para mais informação, dirija-se a Funcionalidades Anti Furto (página 20).

Privacidade de Conta

Verifique se houve fuga de dados nas suas contas online. Para mais informação, dirija-se a Privacidade de conta (página 23).

Bloqueio da aplicação

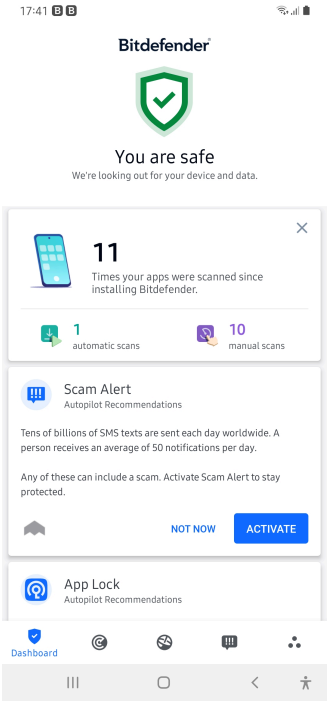
Permite que proteja as suas aplicações instaladas, através da configuração de um código PIN de acesso. Para mais informação, dirija-se a Bloqueio de Aplicativo (página 25).

Relatórios

Mantém um registro de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas à atividade do seu dispositivo. Para mais informações, consulte Relatórios (página 29).

WearON

Comunica com o seu smartwatch para ajudá-lo a encontrar o seu telefone, caso o tenha perdido ou caso se tenha esquecido onde o deixou. Para mais informação, dirija-se a WearON (página 30).


17:41
Bitdefender
You are safe
We're looking out for your device and data.
11
Times your apps were scanned since installing Bitdefender.
1
automatic scans
10
manual scans
Scam Alert
Autopilot Recommendations
Tens of billions of SMS texts are sent each day worldwide. A person receives an average of 50 notifications per day.
Any of these can include a scam. Activate Scam Alert to stay protected.
NOT NOW
ACTIVATE
App Lock
Autopilot Recommendations
Dashboard

3. CARACTERÍSTICAS E FUNCIONALIDADES

3.1. Analisador de Malware

Bitdefender protege o seu aparelho e dados de aplicações maliciosas utilizando a análise na instalação e análise sob pedido.

A interface do Verificador de Malware oferece uma lista de todos os tipos de ameaças analisadas pela Bitdefender, acompanhadas das suas definições. Basta tocar em qualquer ameaça para ver a sua definição.

> **Observação**
> Certifique-se de que o seu dispositivo móvel está ligado à internet. Se o seu dispositivo não estiver ligado à internet, o processo de análise não será iniciado.

- **Verificação na instalação**
  Sempre que instala uma aplicação, o Bitdefender Mobile Security verifica-o automaticamente utilizando a tecnologia na nuvem. O mesmo processo de verificação é iniciado toda vez que as aplicações instaladas são atualizadas.
  Se a aplicação for considerada maliciosa, irá aparecer um alerta solicitando que a desinstale. Toque em **Desinstalar** para aceder ao ecrã de desinstalação da aplicação.
- **Análise a pedido**
  Sempre que quiser saber se as aplicações instaladas no seu dispositivo são seguras para utilização, pode executar uma análise.
  Para iniciar uma análise sob demanda:

  1. Toque em **Verificador de Malware** na barra de navegação inferior.
  2. Toque em **COMEÇAR A ANÁLISE**.

Observação

Permissões adicionais são necessárias no Android 6 para a função do Verificador de Malware. Depois de tocar em **COMEÇAR VARREDURA**, selecione **Permitir** para o seguinte:

- Permitir que o **Antivírus** faça e administre chamadas?
- Permitir que o **Antivírus** aceda a fotos, multimédia e ficheiros no seu dispositivo?

O processo da análise é exibido e poderá interrompê-lo a qualquer momento.

O Bitdefender Mobile Security já vem configurado para analisar o armazenamento interno do seu dispositivo, incluindo qualquer cartão SD ligado. Desta forma, quaisquer aplicações perigosas que estejam no cartão podem ser detetadas antes de causar danos.

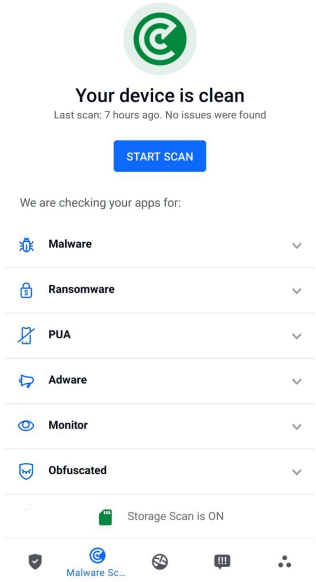
Para desativar a definição Análise do armazenamento:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desative o interruptor **Análise do armazenamento** na área Scanner de Malware.

Caso sejam detetadas quaisquer aplicações maliciosas, serão exibidas informações sobre elas e poderá removê-las tocando no botão **DESINSTALAR**.

O cartão do analisador de Malware exibe o estado do seu dispositivo. Quando está seguro, o cartão fica verde. Quando o dispositivo necessitar de análise ou de alguma ação sua, o cartão ficará vermelho.

Se a sua versão do Android é a 7.1 ou posterior, pode aceder a um atalho para o Verificador de Malware, para poder executar as verificações de forma mais rápida, sem ter de abrir a interface do Bitdefender Mobile Security. Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .



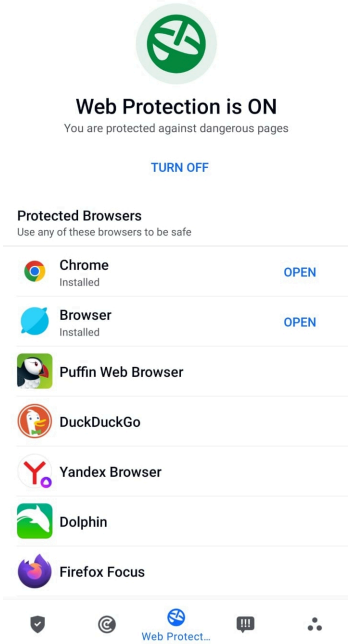
3.2. Proteção da Internet

A Proteção na Web verifica ao utilizar o Bitdefender páginas web de serviços em nuvem que você acede com o navegador padrão do Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser e Dolphin.

Observação

São necessárias permissões adicionais no Android 6 para a função Web Protection.

Ative a permissão para registar como serviço de Acessibilidade e pressione **LIGAR** quando solicitado. Toque em **Antivírus** e ative o botão, depois confirme que concorda com o acesso às permissões do seu dispositivo.



Cada vez que acede a um site bancário, a Proteção na Web da Bitdefender é configurada para notificá-lo para utilizar o Bitdefender VPN. A notificação aparece na barra de estado. Recomendamos a utilização do Bitdefender VPN enquanto estiver conectado à sua conta bancária, para que os seus dados possam ficar a salvo de possíveis violações de segurança.

Para desativar a notificação Proteção Web:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue o interruptor correspondente na área de Proteção Web.

3.3. 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 se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o VPN, pode 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.

Há duas formas de ativar ou desativar o Bitdefender VPN:

- Toque em **LIGAR** na placa VPN do Painel.
  O estado do Bitdefender VPN é exibido.
- Toque em **VPN** na barra de navegação inferior e, em seguida, toque em **CONECTAR**.
  Pressione **CONECTAR** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fios não seguras.
  Pressione **DESCONECTAR** quando desejar desativar a ligação.

> **Observação**
> Na primeira vez que ligar o VPN, deve permitir a solicitação do Bitdefender para configurar uma ligação VPN que monitorizará o tráfego de rede. Prima **OK** para continuar.

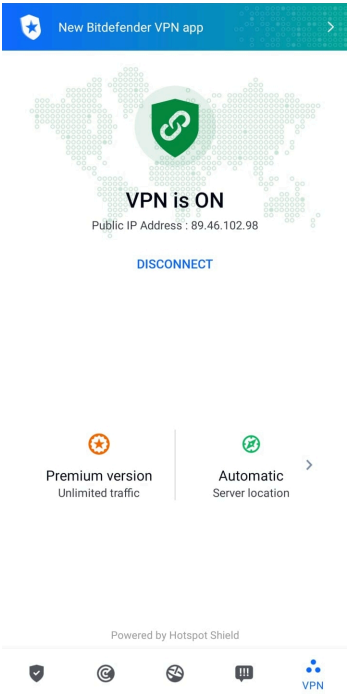
Se a versão do seu Android for 7.1 ou superior, pode aceder a um atalho para o Bitdefender VPN, sem abrir a interface do Bitdefender Mobile Security.

Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .

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 Localização do servidor na ferramenta de VPN e, em

seguida, selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a



3.3.1. Definições da VPN

Para uma configuração avançada da sua VPN:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.

Nas área VPN, pode configurar as seguintes opções:

- Acesso rápido ao VPN - uma notificação aparecerá na barra de estado do seu dispositivo permitindo que ligue o VPN rapidamente.
- Alerta de Wi-Fi aberto - sempre que se ligar a uma rede Wi-Fi aberta, a barra de estado do seu dispositivo vai pedir-lhe para utilizar o VPN.

3.3.2. Assinaturas

O Bitdefender VPN oferece gratuitamente uma cota de tráfego diária de 200 MB por dispositivo para garantir a sua ligação sempre que precisar, ao ligá-lo automaticamente à localização ideal do 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 para a versão do Bitdefender Premium VPN a qualquer momento tocando em **Ativar Premium** na janela do VPN.

A subscrição do Bitdefender Premium VPN é independente da subscrição do Bitdefender Mobile Security, o que significa que poderá utilizá-la enquanto estiver disponível, independentemente do estado da sua subscrição de segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas a do Bitdefender Mobile Security ainda estiver ativa, será revertido para o plano gratuito.

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

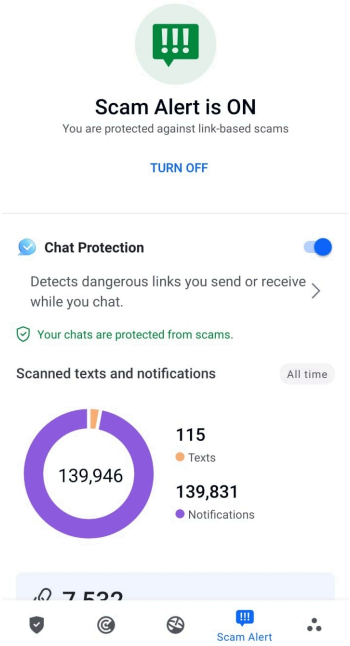
> **Observação**
> O Bitdefender VPN também funciona como uma aplicação autónoma em todos os sistemas operativos suportados, incluindo Windows, macOS, Android e iOS.

3.4. Scam Alert

A funcionalidade Scam Alert toma medidas preventivas em primeiro plano, lidando com situações potencialmente perigosas antes mesmo que elas tenham a oportunidade de se tornar um problema, incluindo ameaças de malware. O Scam Alert monitoriza todas as mensagens SMS recebidas e notificações do Android em tempo real.

Quando um link perigoso chegar por mensagem no seu telefone, um aviso irá aparecer no seu ecrã. A Bitdefender irá oferecer duas opções. A primeira opção é ignorar a informação. A segunda opção é **VISUALIZAR DETALHES**. Isso fornece mais informações sobre o incidente, bem como conselhos essenciais, como por exemplo:

- Não abra ou encaminhe o link detetado.
- No caso dos SMS, elimine a mensagem, se possível.
- Bloqueie o remetente se não for um contacto de confiança.
- Elimine a aplicação que envia links perigosos em notificações.



Observação

Devido a limitações do sistema operativo Android, a Bitdefender não pode apagar mensagens de texto ou tomar quaisquer medidas diretas relacionadas com as mensagens SMS, ou qualquer outra fonte de notificações maliciosas. Se ignorar o aviso de Scam Alert e tentar abrir um link perigoso, a funcionalidade da Proteção na Web da Bitdefender captura-o automaticamente, ao impedir que o seu dispositivo seja infetado.

3.4.1. Ativar o Scam Alert

Para ativar o Scam Alert, é necessário conceder o acesso às mensagens SMS e ao sistema de notificação à aplicação da Bitdefender Mobile Security:

1. Abra a aplicação do Bitdefender Mobile Security instalado no seu telefone ou tablet Android.
2. No ecrã principal da aplicação da Bitdefender, toque na opção **Scam Alert** na barra de navegação inferior, depois toque em **ATIVAR**.
3. Toque no botão **PERMITIR**.
4. Na lista de Acesso à Notificação, mude o Bitdefender Security para a posição **ON**.
5. Confirme a ação ao tocar em **PERMITIR**.
6. Volte ao ecrã de Scam Alert e toque em **PERMITIR** para dar ao Bitdefender a capacidade de verificar as mensagens SMS recebidas.

3.4.2. Proteção de chat em tempo real

As mensagens de chat são o nosso meio mais confortável de manter contacto, mas são também uma forma fácil para que links perigosos cheguem até si.

Com o recurso de Proteção de Chat ativo, o módulo Scam Alert vai além da proteção das suas mensagens de texto e notificações para manter os seus chats seguros também contra ataques baseados em links, ao detetar os links perigosos que envia ou recebe durante o chat.

Para ativar a Proteção de Chat:

1. Abra o aplicativo Bitdefender Mobile Security instalado em seu telefone ou tablet Android.
2. No ecrã principal da aplicação da Bitdefender, toque na opção **Scam Alert** na barra de navegação inferior.
3. Verá a funcionalidade de Proteção de Chat no topo da aba do Scam Alert. Mude o interruptor correspondente para a posição **ON**.

> **Observação**
> Atualmente, a Proteção de Chat é compatível com as seguintes aplicações:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

3.5. Funcionalidades Anti Furto

Bitdefender pode ajudá-lo a localizar o seu dispositivo e impedir que os seus dados pessoais caiam nas mãos erradas.

Tudo o que necessita de fazer é ativar o Anti-roubo a partir do dispositivo e, quando necessário, aceder à **Bitdefender Central** a partir de qualquer Web browser, em qualquer lugar.

> **Observação**
> A interface do Antifurto também inclui uma hiperligação para a nossa aplicação da Central Bitdefender no Google Play Store. Pode utilizar esta hiperligação para transferir a aplicação, caso ainda não o tenha feito.

O Bitdefender Mobile Security oferece as seguintes características Antifurto:

Localização remota

Visualize a localização atual do seu dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Bloqueio remoto

Bloqueie o ecrã do seu dispositivo e defina uma palavra-passe para desbloquear o mesmo.

Limpeza remota

Remova todos os dados pessoais do seu dispositivo roubado.

Enviar alerta para o dispositivo (Scream)

Envie uma mensagem remotamente para ser exibida no ecrã do dispositivo ou para emitir um som alto no altifalante do dispositivo.

Caso venha a perder o seu dispositivo, pode informar a quem o encontrar como pode ser devolvido, exibindo uma mensagem no ecrã do dispositivo.

Caso tenha perdido o seu dispositivo e exista a possibilidade de não estar longe de si (por exemplo, em algum lugar em casa ou no escritório), que melhor maneira de encontrá-lo do que fazê-lo tocar um som alto? O som será reproduzido mesmo se o dispositivo estiver no modo silencioso.

3.5.1. A ativar o Anti Furto

Para ativar a função Anti Furto, basta completar o processo de configuração do cartão Anti Furto disponível no Painel de Controlo.

Também pode ativar a função Anti Furto seguindo estas instruções:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Antifurto**.
3. Toque em **ATIVAR**.
4. O seguinte procedimento será iniciado para ajudá-lo na ativação desta função:

   Observação
   São necessárias permissões adicionais no Android 6 para a função Anti Furto.

   Para o ativar, siga estes passos:

   a. Toque em **Ativar Antifurto** e, em seguida, toque em **ATIVAR**.

   b. Permite que o **Antivírus** aceda à localização deste dispositivo

   a. **Conferir Privilégios de Administrador**
   Estes privilégios são essenciais para o funcionamento da função Anti Furto e devem ser concedidas antes de continuar.

   b. **Definir o PIN da Aplicação**
   Para evitar o acesso não autorizado ao seu dispositivo, tem de definir um código PIN. Sempre que for feita uma tentativa de acesso ao seu dispositivo, é necessário introduzir o PIN primeiro.

Em alternativa, nos dispositivos que suportam a autenticação com impressão digital, pode utilizar uma confirmação de impressão digital em vez do código PIN configurado.
O mesmo código PIN é utilizado pelo Bloqueio de Aplicação para proteger as suas aplicações instaladas.

c. **Ativar Foto Instantânea**
Sempre que alguém tentar desbloquear o seu dispositivo sem sucesso enquanto Tirar Foto estiver ativado, o Bitdefender tira uma foto.
Dokładniej, za każdym razem, gdy kod PIN, hasło lub potwierdzenie odcisku palca, które ustawiłeś, aby chronić urządzenie, jest trzykrotnie błędnie wpisane, robione jest zdjęcie przy użyciu przedniego aparatu. A foto é guardada com o carimbo de data/hora e o motivo e pode ser vista quando abre Bitdefender Mobile Security da janela Antirroubo.
Alternatywnie można wyświetlić zrobione zdjęcie w koncie Bitdefender:

i. Vá para: https://central.bitdefender.com.
ii. Aceda à sua conta.
iii. Selecione os **Meus dispositivos** painel.
iv. Selecione o dispositivo Android e o separador **Antirroubo**.
v. Toque em ⋮ ao lado de **Verificar suas fotos** para ver as últimas fotografias que foram tiradas.
Só são guardadas as duas fotografias mais recentes.

Ao ativar o recurso Anti-roubo, pode ativar ou desativar os comandos de Controlo Web de maneira individual na janela de Anti-roubo tocando nas opções correspondentes.

3.5.2. Usar as funcionalidades Anti-Roubo a partir da Bitdefender Central

> **Observação**
> Todas as funcionalidades de Anti Furto necessitam que a opção **Dados em segundo plano** esteja ativa nas configurações de Dados do seu dispositivo.

Para aceder às funções anti-furto da sua conta Bitdefender:

1. Aceda a **Central da Bitdefender**.
2. Selecione os **Meus dispositivos** painel.
3. Na janela **OS MEUS DISPOSITIVOS**, selecione o cartão de dispositivo desejado tocando no botão **Ver detalhes** correspondente.
4. Selecione o separador **Anti Furto**.
5. Toque no botão correspondente à funcionalidade que pretende utilizar:
   Localizar - exibe a localização do seu dispositivo no Google Maps.
   MOSTRAR IP - exibe o último endereço de IP para o dispositivo selecionado.
   Alerta - escreva uma mensagem para ser exibida no ecrã do seu dispositivo e/ou para fazer com que o seu dispositivo emita um alarme sonoro.
   Bloqueio - bloqueie o seu dispositivo e defina um código PIN para desbloqueá-lo.
   Limpeza - apague todos os dados do seu dispositivo.

   > **Importante**
   > Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

3.5.3. Funcionalidades Antirroubo

Se pretender ativar ou desativar os comandos remotos:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Anti-roubo**.
3. Ative ou desative as opções pretendidas.

3.6. Privacidade de conta

O Bitdefender Account Privacy deteta se houve alguma violação de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. 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.

A novas verificações automáticas são definidas para serem executadas em segundo plano, mas é possível executar análises manuais diariamente.

As notificações serão apresentadas sempre que são detetadas novas quebras que incluam qualquer uma das contas de e-mail validadas.

Para começar a proteger informações pessoais:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Privacidade da conta**.
3. Toque em **INICIAR**.
4. O endereço de e-mail utilizado para criar a sua conta da Bitdefender aparece e é automaticamente adicionado à lista de contas monitorizadas.
5. Para adicionar outra conta, toque em **ADICIONAR CONTA** na janela de Privacidade da Conta e escreva o endereço de e-mail.
   Toque em **ADICIONAR** para continuar.
   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.
   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 quebras 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) quebra(s) identificada(s) como Resolvido. Para tal:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Privacidade da conta**.
3. Toque na conta que acabou de proteger.
4. Toque na quebra de onde protegeu a conta.
5. Toque em **RESOLVIDO** para confirmar que a conta está protegida.

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

Para parar de ser notificado sempre que são realizadas análises automáticas:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue o interruptor correspondente na área Privacidade da conta.

3.7. Bloqueio de Aplicativo

Aplicações instaladas, como e-mails, fotos ou mensagens, podem conter dados pessoais que gostaria que permanecessem privados, limitando o acesso a estes de forma seletiva.

O Bloqueio de Aplicação ajuda-o a bloquear o acesso indesejado às aplicações, através da configuração de um código PIN de acesso de segurança. O código PIN deve ter no mínimo 4 dígitos e no máximo 8 e será solicitado sempre que pretender aceder às aplicações restritas.

A autenticação biométrica (tal como confirmação de impressão digital ou reconhecimento facial) pode ser utilizada em vez do código PIN configurado.

3.7.1. A ativar o Bloqueio de Aplicação

Para restringir o acesso a aplicações específicas, configure o Bloqueio de Aplicação através do cartão exibido no Painel de Controlo após a ativação da função Anti Furto.

Também pode ativar o Bloqueio de Aplicação seguindo estas instruções:

1. Tocar **Mais** na barra de navegação inferior.

2. Toque em **Bloqueio de aplicações**.
3. Tocar **LIGAR**.
4. Permitir o acesso aos dados de utilização para o Bitdefender Security.
5. Permitir **prioridade em relação a outras aplicações**.
6. Volte à aplicação, configure o código de acesso e pressione **DEFINIR PIN**.

> **Observação**
> Este passo será apenas necessário se não tiver configurado o PIN na função Anti Furto.

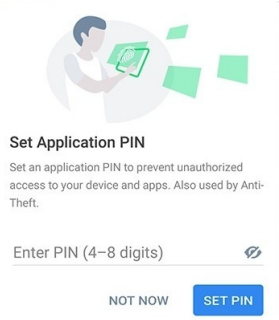
7. Permite que a opção Tirar Foto apanhe qualquer intruso que tente aceder aos seus dados pessoais.

> **Observação**
> São necessárias permissões adicionais no Android 6 para a função Tirar Foto. Para ativá-la, permita que o **Antivírus** tire fotos e grave vídeos.

8. Selecione as aplicações que gostaria de proteger.

Utilizar o PIN ou a impressão digital errada cinco vez seguidas ativará uma pausa de 30 segundos. Dessa forma, qualquer tentativa de aceder às aplicações protegidas será bloqueada.

> **Observação**
> O mesmo código PIN é utilizado pelo Anti Furto para ajudá-lo a localizar o seu dispositivo.



3.7.2. MODO DE BLOQUEIO

A primeira vez que adicionar uma aplicação ao Bloqueio de aplicação, o ecrã Modo de bloqueio de aplicação aparece. Daqui é possível escolher quando a função Bloqueio de aplicação deve proteger as aplicações intaladas no seu dispositivo.

Pode selecionar entre uma das seguintes opções:

- **Necessita sempre de desbloqueio** - sempre que as aplicações bloqueadas são acedidas, o código PIN ou impressão digital que configurou será utilizado.
- **Manter desbloqueado até o ecrã apagar** - o acesso às suas aplicações será válido até o ecrã apagar.
- **Bloquear após 30 segundos** - é possível sair e aceder novamente às suas aplicações desbloqueadas num espaço de 30 segundos.

Caso pretenda alterar a definição selecionada:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque em **Requer sempre desbloqueio** na área Bloqueio de aplicação.
4. Escolha a opção desejada.

3.7.3. Definições do Bloqueio de Aplicação

Para uma configuração avançada do Bloqueio de aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.

Na área Bloqueio de aplicação, é possível configurar as opções seguintes:

- **Sugestão de aplicação confidencial** - receba uma notificação de bloqueio sempre que instalar uma aplicação confidencial.
- **Requer sempre desbloqueio** - escolha uma das opções de bloqueio e desbloqueio disponíveis.
- **Desbloqueio inteligente** - mantenha as aplicações desbloqueadas enquanto estiver ligado a redes Wi-Fi de confiança.

- **Teclado aleatório** - previne a leitura do PIN ao mostrar os números de forma aleatória.

3.7.4. Tirar foto

Com o Bitdefender Snap Photo, pode apanhar os seus amigos ou parentes rapidamente. Desta forma, pode educar os olhos curiosos deles para não passarem os olhos pelos seus ficheiros pessoais ou pelas aplicações que utiliza.

A função funciona de forma fácil: sempre que o código PIN ou a confirmação por impressão digital que definiu para proteger as suas aplicações for inserido de forma errada três vezes seguidas, será tirada uma foto com a câmara frontal. A foto será guardada com a informação sobre o dia, hora e motivo, e poderá ser visualizada quando abrir o Bitdefender Mobile Security e aceder à função do Bloqueio de Aplicação.

> **Observação**
> Esta função está disponível apenas para telefones que têm uma câmara frontal.

Para configurar a função de Instantâneo para Bloqueio de aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Ative o interruptor correspondente na área Instantâneo.

As fotos tiradas quando é introduzido o PIN incorreto são exibidas na janela de Bloqueio de Aplicação e podem ser visualizadas em ecrã completo.

De forma alternativa, eles podem ser vistos na sua conta Bitdefender:

1. Vá para: https://central.bitdefender.com.
2. Faça login em sua conta.
3. Selecione o painel **Os meus dispositivos**.
4. Selecione seu dispositivo Android e, em seguida, o **Anti-roubo** aba.
5. Tocar ao lado de **Verifique seus instantâneos** para ver as fotos mais recentes que foram tiradas.

Apenas as duas fotos mais recentes são salvas.

Para parar o carregamento de fotos tiradas na sua conta Bitdefender:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desative **Carregar fotos** na área Instantâneo.

3.7.5. Desbloqueio Inteligente

Um método fácil para que a função Desbloqueio de Aplicação deixe de solicitar o código PIN ou a confirmação por impressão digital para as aplicações protegidas sempre que acede é ativar o Desbloqueio Inteligente.

Com o Desbloqueio Inteligente pode configurar as redes Wi-Fi que costuma utilizar como fiáveis e quando estiver ligado a elas, as definições de bloqueio do Bloqueio de Aplicação serão desativadas para as aplicações protegidas.

Para configurar a função Desbloqueio inteligente:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Bloqueio do aplicativo**.
3. Toque no botão .
4. Toque no interruptor ao lado do **Smart Unlock**, caso a funcionalidade ainda não esteja ativada
   Valide utilizando a sua impressão digital ou o seu PIN.
   A primeira vez que ativar a funcionalidade, deverá ativar a permissão de localização. Toque no botão **PERMITIR** e, em seguida, prima **PERMITIR** novamente.
5. Toque em **ADICIONAR** para configurar a ligação Wi-Fi que está a utilizar atualmente como sendo de confiança.

Sempre que mudar de opinião, desative a função e as redes Wi-Fi que configurou como fiáveis serão tratadas como não fiáveis.

3.8. Relatórios

O recurso Relatórios mantém um registo detalhado de eventos relacionados com a atividade de análise do seu dispositivo.

Sempre que acontecer algo relevante para a segurança do seu dispositivo, será adicionada uma nova mensagem aos Relatórios.

Para aceder à secção Relatórios:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

Os seguintes separadores estão disponíveis na janela Relatórios:

- **RELATÓRIOS SEMANAIS** - aqui tem acesso ao estado de segurança e às tarefas executadas da semana atual e anterior. O relatório semanal é gerado todos os domingos e receberá uma notificação informando-o acerca da sua disponibilidade.
  Todas as semanas será exibida uma nova dica nesta secção, então lembre-se de conferir regularmente para obter o máximo do que a sua aplicação pode oferecer.
  Para parar de receber notificações sempre que um relatório é gerado:
  1. Tocar **Mais** na barra de navegação inferior.
  2. Tocar **Configurações**.
  3. Desative o interruptor **Notificação de novo relatório** na área Relatórios.
- **REGISTO DE ATIVIDADES** - aqui poderá aceder a informações detalhadas sobre as atividades da sua aplicação Bitdefender Mobile Security, desde quando foi instalada no seu dispositivo Android.
  Para eliminar o relatório de atividade disponível:
  1. Tocar **Mais** na barra de navegação inferior.
  2. Tocar **Configurações**.
  3. Toque em **Apagar registo de atividades**, e depois toque em **APAGAR**.

3.9. WearON

Com Bitdefender WearON, pode encontrar facilmente o seu smartphone, esteja ele na sala de reunião do escritório ou sob uma almofada no sofá. O dispositivo pode ser encontrado mesmo se o modo silencioso estiver ativado.

Mantenha esta função ativada para garantir que terá sempre o seu smartphone por perto.

Observação
A função funciona com Android 4.3 e Android Wear.

3.9.1. A ativar o WearON

Para utilizar o WearON, só precisa de ligar o seu smartwatch à aplicação do Bitdefender Mobile Security e ativar a função com o seguinte comando de voz:

Início:<Onde está o meu telefone>

O **Bitdefender WearON** tem dois comandos:

1. **Alerta de telefone**
   Com o recurso Alerta do Telefone encontra rapidamente o seu smartphone, sempre que se afastar muito dele.
   Se estiver com o seu smartwatch, ele detectará automaticamente a aplicação no seu telefone e irá vibrar sempre que estiver muito longe do seu relógio, mais precisamente, quando a ligação de Bluetooth for perdida.
   Para ativar esta função, abra o Bitdefender Mobile Security, toque em **Configurações Globais** no menu e selecione o botão correspondente na secção WearON.
2. **Grito**
   Encontrar o seu telefone nunca foi tão fácil. Quando se esquecer onde deixou o seu telefone, toque no comando Apitar no seu relógio para fazer o seu telefone apitar.

3.10. Sobre

Para mais informações sobre a versão do Bitdefender Mobile Security que tem instalada, para aceder e ler o Acordo de subscrição e Política de privacidade, e visualizar as licenças Open-source:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque na opção desejada na área Sobre.

4. SOBRE A CENTRAL BITDEFENDER

A Central Bitdefender é a plataforma onde tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que a Bitdefender estiver instalada. Pode aceder à sua conta da Bitdefender de qualquer computador ou dispositivo móvel ligado à internet, acedendo a https://central.bitdefender.com, ou diretamente pela 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 for Android
  - Bitdefender Mobile Security for iOS
  - A linha de produtos da Bitdefender para Windows
  - Bitdefender Antivirus for Mac
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.
- Proteja os dispositivos de rede e os seus dados contra roubo ou perda com o Anti-Roubo.

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 para: 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 tem instalado.

  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. Toque no ícone no lado superior direito do ecrã.
3. Toque em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Tocar **INICIAR**.
   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. Toque 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.
  Toque em **CONTINUAR**.

  c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, toque 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. Toque 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. Toque 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. Toque 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 a 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. Toque em **Dispositivos de confiança**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Toque no dispositivo pretendido.

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 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

Porque é que o Bitdefender Mobile Security requer uma ligação à Internet?

A aplicação precisa de comunicar com os servidores do Bitdefender para determinar o estado de segurança das aplicações que analisa e das páginas web que visita e também para receber os comandos da sua conta Bitdefender quando utilizar a função Anti Furto.

Para que é que o Bitdefender Mobile Security precisa de cada permissão?

- Acesso à internet -> utilizado para comunicação com a nuvem.
- Ler o estado e a identidade do telefone -> utilizado para detetar se o dispositivo está ligado à internet e extrair certas informações do dispositivo necessárias para criar uma identificação única ao comunicar com a nuvem da Bitdefender.
- Ler e escrever marcadores do navegador -> O módulo Proteção da Web apaga sites maliciosos do seu histórico de navegação.
- Ler os dados de registo -> O Bitdefender Mobile Security deteta vestígios de atividades de ameaças a partir dos registos do Android.
- Localização -> necessária para a localização remota.
- Câmera -> necessária para Tirar foto.
- Armazenamento -> utilizado para permitir que o Analisador de Malware verifique o cartão SD.

Como é que posso parar de submeter informações de Bitdefender sobre aplicações suspeitas?

Por predefinição, o Bitdefender Mobile Security envia relatórios aos servidores Bitdefender sobre aplicações suspeitas que esteja a instalar. Estas informações são essenciais para melhorar a deteção de ameaças e pode ajudar-nos a oferecer-lhe uma melhor experiência no futuro. Caso queira parar de nos enviar informações sobre aplicações suspeitas:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Desligue **Deteção dentro da nuvem** na área Scanner de Malware.

Onde posso ver mais informações sobre a atividade do aplicação?

O Bitdefender Mobile Security mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder, consulte a atividade da aplicação:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Relatórios**.
   Na janela de RELATÓRIOS SEMANAIS, é possível aceder aos relatórios que foram gerados todas as semanas e na janela REGISTO DE ATIVIDADE, pode visualizar as informações sobre a atividade da sua aplicação Bitdefender.

Esqueci-me do código PIN que defini para proteger a minha aplicação. O que devo fazer?

1. Acesso Bitdefender Central.
2. Selecione os **Meus dispositivos** painel.
3. Toque no cartão de dispositivo pretendido e, em seguida, toque em no canto superior direito do ecrã.
4. Selecione **Configurações**.
5. Recupere o PIN no campo **PIN da Aplicação**.

Como é que posso alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo?

Se pretende alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Configurações**.
3. Toque em **CÓDIGO PIN** de segurança na área Antirroubo.
4. Introduza o código PIN atual.
5. Introduza o novo código PIN que pretende definir.

Como posso desligar a função Bloqueio de Aplicação?

Não há qualquer opção para desligar a função Bloqueio de Aplicação, mas pode desativá-la facilmente ao desmarcar as caixas próximas às aplicações selecionadas depois que validar o PIN ou impressão digital definida.

Como posso definir outra rede sem fios como fiável?

Em primeiro, tem de ligar o seu dispositivo à rede sem fios que pretende definir como de confiança. Em seguida, siga estes passos:

1. Tocar **Mais** na barra de navegação inferior.
2. Tocar **Bloqueio do aplicativo**.
3. Toque em no canto superior direito.
4. Toque em **ADICIONAR** ao lado da rede que pretende definir como de confiança.

Como posso parar de ver fotografias associadas tiradas nos meus dispositivos?

Para parar de tornar visíveis as fotografias associadas tiradas nos seus dispositivos:

1. Acesso Bitdefender Central.
2. Toque em no canto superior direito do ecrã.
3. Toque em **Definições** no menu deslizante.
4. Desative a Opção **Mostrar/Não mostrar fotos instantâneas tiradas nos seus dispositivos**.

Como posso manter as minhas compras online seguras?

As compras online têm riscos elevados quando alguns detalhes são ignorados. Para não ser vítima de fraude, recomendamos o seguinte:

- Matenha a aplicação de segurança atualizada.
- Efetue pagamentos online apenas com proteção do comprador.
- Utilize uma VPN ao estabelecer ligação com a internet a partir de redes sem fios não protegidas e públicas.
- Preste atenção às palavras-passe que atribuiu às suas contas online. Têm de ser fortes e incluir letras maiúsculas e minúsculas, números e símbolos (@, !, %, #, etc.).
- Certifique-se de que as informações são enviadas por ligações seguras. A extensão do site Web online tem de ser HTTPS:// e não HTTP//.

Quando devo utilizar o Bitdefender VPN?

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

O Bitdefender VPN terá um impacto negativo na bateria do meu dispositivo?

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios não seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

Posso alterar a conta da Bitdefender ligada ao meu dispositivo?

Sim, pode alterar facilmente a conta Bitdefender associada ao seu dispositivo seguindo estes passos:

1. Tocar **Mais** na barra de navegação inferior.
2. Toque no seu endereço de e-mail.
3. Toque em **Terminar sessão na sua conta**. Se tiver sido definido um código PIN, será solicitado a inseri-lo.

4. Confirme sua escolha.
5. Escreva o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes e, em seguida, toque em **ENTRAR**.

Como o Bitdefender Mobile Security influencia o desempenho e a bateria do meu aparelho?

O impacto é muito baixo. A aplicação só é executada quando é fundamental — inclusive durante a instalação e quando navega pela interface da aplicação — ou quando pretende realizar uma verificação de segurança. O Bitdefender Mobile Security não funciona em plano de fundo quando liga para amigos, envia mensagens ou joga.

O que é o Administrador de Dispositivos?

O Administrador de Dispositivos é um recurso do Android que dá ao Bitdefender Mobile Security as permissões necessárias para executar certas tarefas remotamente. Sem estes privilégios, o bloqueio remoto não funcionaria e a limpeza do dispositivo não seria capaz de remover completamente os seus dados. Se quiser remover aplicação, certifique-se de revogar estes privilégios antes de tentar desinstalar em **Configurações > Segurança > Selecionar administradores dos dispositivos**.

Como resolver o erro "Sem token Google" que aparece quando inicia a sessão no Bitdefender Mobile Security.

Este erro ocorre quando o dispositivo não está associado a uma conta Google, ou está associado, mas um problema temporário está a evitar que se ligue ao Google. Tente uma das seguintes soluções:

- Vá às Definições do Android > Aplicações > Gerir aplicações > Bitdefender Mobile Security e toque em **Apagar dados**. Depois tente entrar novamente.
- Certifique-se de que o seu dispositivo está associado a uma conta Google.
  Para verificar isso, vá a Definições > Contas e sincronização e veja se uma conta do Google aparece listada em **Gerir contas**. Adicione a sua conta se uma não estiver listada, reinicie o seu dispositivo e depois tente entrar no Bitdefender Mobile Security.
- Reinicie o seu dispositivo e, em seguida, tente iniciar sessão novamente.

Em quais idiomas o Bitdefender Mobile Security está disponível?

O Bitdefender Mobile Security está atualmente disponível nos seguintes idiomas:

- Brasileiro
- Checo
- Holandês
- Inglês
- Francês
- German
- Grego
- Húngaro
- Italiano
- Japonês
- Coreano
- Polaco
- Português
- Romanian
- Russo
- Spanish
- Sueco
- Tailandês
- Turco
- Vietnamita

Outros idiomas serão acrescentadas em futuros lançamentos. Para alterar o idioma da interface do Bitdefender Mobile Security, vá a Definições **Idiomas e teclado**, no seu dispositivo e defina o idioma que pretende utilizar no dispositivo.

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 48).

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.