

SOFTWARE MALICIOSO EM DISPOSITIVOS MÓVEIS

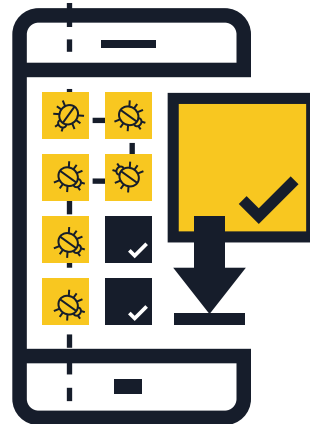


SUGESTÕES E CONSELHOS PARA SE PROTEGER



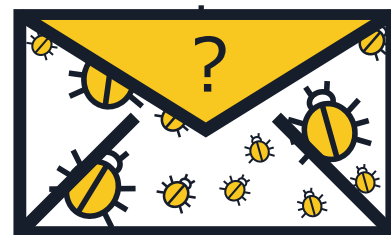
1 Instale aplicações apenas de fontes seguras

- **Adquira os produtos em lojas de aplicações conceituadas** — Antes de descarregar uma aplicação, investigue tanto a aplicação como os seus criadores. Cuidado com as hiperligações enviadas por e-mail e mensagens de texto; estas podem induzi-lo a instalar aplicações enganadoras de terceiros ou fontes desconhecidas.
- **Verifique as críticas e classificações de outros utilizadores**, se estiverem disponíveis.
- **Leia as permissões da aplicação** — Verifique os tipos de dados a que a aplicação pode aceder e se esta pode partilhar a sua informação com terceiros. Se desconfiar dos termos e condições ou não estiver totalmente de acordo com os mesmos, não descarregue a aplicação.



2 Não clique em hiperligações ou anexos de e-mails e mensagens de texto não solicitados

- **Não confie em hiperligações de e-mails e mensagens de texto não solicitados** (SMS e MMS) — Elimine-os assim que os receber.
- **Verifique bem URL e códigos QR abreviados** — Podem estar ligados a sites Web prejudiciais ou descarregar diretamente software malicioso para o seu dispositivo. Antes de clicar, utilize um site de pré-visualização de URL para confirmar a legitimidade do endereço Web. Antes de digitalizar um código QR, escolha um leitor de QR pré-visualização do endereço Web incorporado e utilize um software de segurança para dispositivos móveis que o alerte para as hiperligações perigosas.



3 Termine a sessão nos sites Web depois de efetuar pagamentos

- **Nunca guarde nomes de utilizador e palavras-passe no browser ou nas aplicações do seu dispositivo móvel** — Se perder ou roubarem o seu telemóvel ou tablet, qualquer pessoa poderá ter acesso às suas contas. Assim que a transação estiver concluída, termine a sessão no site, em vez de fechar apenas o browser.
- **Não aceda à sua conta bancária nem faça compras online utilizando ligações Wi-Fi públicas** — Faça operações bancárias e transações online só a partir de redes que conhece e em que confia.
- **Verifique bem a URL do site** — Antes de iniciar a sessão ou enviar informação sigilosa, certifique-se de que o endereço Web está correto. Pondere descarregar a aplicação oficial do seu banco para garantir que está sempre ligado ao verdadeiro site.

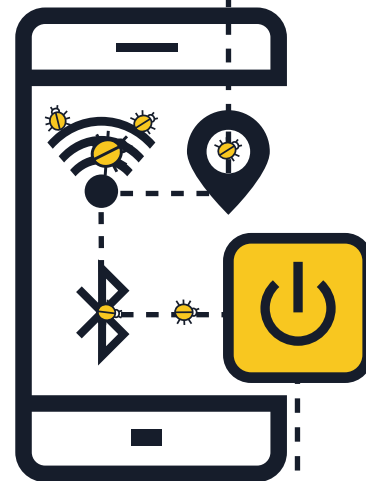


4 Mantenha o sistema operativo e as aplicações atualizados

- **Descarregue as atualizações de software do seu dispositivo móvel sempre que tal seja solicitado** — A instalação das atualizações mais recentes garante não só uma maior proteção do dispositivo, como também um melhor desempenho do mesmo.

5 Desligue o Wi-Fi, os serviços de localização e o Bluetooth, se não estiverem a ser utilizados

- **Se não estiver a utilizar o Wi-Fi, desligue-o** — Os criminosos cibernéticos podem aceder à sua informação se a ligação não for segura. Se possível, utilize uma ligação de dados 3G ou 4G em vez de hotspots. Pode ainda optar pelo serviço de uma rede privada virtual (VPN) para manter os seus dados encriptados quando estiverem em trânsito.
- **Não permita que as aplicações utilizem os seus serviços de localização, a não ser que seja necessário** — Esta informação pode ser partilhada ou divulgada e utilizada para ativar anúncios com base na sua localização.
- **Quando não precisar do Bluetooth, desligue-o** — Certifique-se de que está totalmente desligado e não apenas no modo invisível. É frequente os dispositivos virem predefinidos de fábrica, de modo a permitir que outros se liguem a eles sem que tenha conhecimento. Os utilizadores mal-intencionados podem copiar os seus ficheiros, aceder a outros dispositivos ligados ao seu ou até aceder remotamente ao seu telemóvel para efetuar chamadas e enviar mensagens de texto, encarecendo a sua fatura.



6 Evite fornecer informação pessoal

- **Nunca forneça dados pessoais** na resposta a mensagens de texto ou e-mails que aleguem ser do seu banco ou de outra empresa legítima. Em vez disso, contacte a entidade diretamente para confirmar o pedido em causa.
- **Reveja regularmente a fatura do seu dispositivo móvel para verificar se existe alguma cobrança suspeita** — Se identificar despesas que não tenha feito, contacte imediatamente o seu prestador de serviços.

7 Não faça jailbreak no seu dispositivo

- O jailbreak é o processo de remoção dos limites de segurança impostos pelo fornecedor do sistema operativo, obtendo acesso total ao sistema operativo e às funções do dispositivo. **Se fizer jailbreak no seu próprio dispositivo, pode reduzir drasticamente a respetiva segurança**, abrindo brechas na segurança que podem não ser tão óbvias.

8 Faça uma cópia de segurança dos seus dados

- **Muitos smartphones e tablets têm capacidade para criar uma cópia de segurança no modo sem fios** — Consulte as opções do sistema operativo do seu dispositivo. Ao criar uma cópia de segurança do smartphone ou tablet, poderá recuperar facilmente os seus dados pessoais em caso de perda, roubo ou danos no dispositivo.



9 Instale uma aplicação de segurança móvel

- Todos os sistemas operativos correm o risco de serem infetados. Se estiver disponível, **recorra a uma solução de segurança móvel** que detete e evite software malicioso, spyware e aplicações malignas, além de incluir outras funções de privacidade e antirroubo.

