APPS

É SÓ UM JOGO?

Instale apenas aplicações de lojas de aplicações oficiais

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.

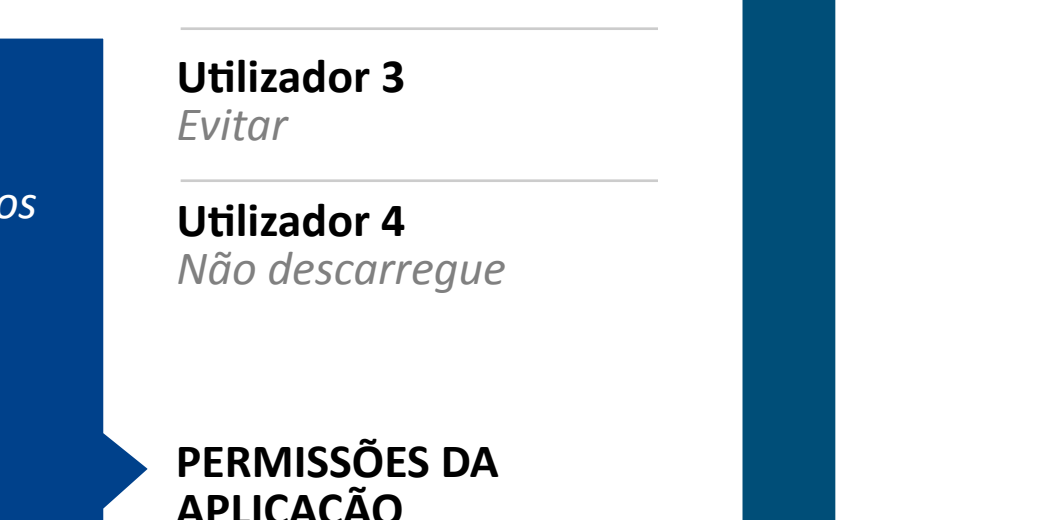
VERIFIQUE AS CRITICAS E CLASSIFICAÇÕES DE OUTROS UTILIZADORES

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. Necessita de todas estas permissões? Se não, não descarregue.

INSTALE UMA APLICAÇÃO DE SEGURANÇA MÓVEL

Examinará todas as aplicações do seu dispositivo e todas as que instalar posteriormente, alertando-o em caso de deteção de software malicioso.



EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware

SOFTWARE MALICIOSO DE SERVIÇO BANCÁRIO MÓVEL

O SOFTWARE MALICIOSO PODE SAIR-LHE CARO

O software malicioso de serviços bancários móveis foi concebido para roubar a informação financeira armazenada no seu dispositivo.

COMO SE PROPAGA?

Ao visitar sites Web nocivos

Ao descarregar aplicações nocivas

Através do phishing

QUAIS SÃO OS RISCOS?

Recolha da sua informação de autenticação pessoal

Levantamentos não autorizados

O QUE PODE FAZER?

Descarregue a aplicação móvel oficial do seu banco e certifique-se sempre de que está a visitar o site Web verdadeiro do banco.

Se perder o seu telemóvel ou mudar de número, contacte o seu banco para que possam atualizar a sua informação.

Evite que o site ou a aplicação online do seu banco inicie a sua sessão automaticamente.

Não partilhe qualquer informação sobre a sua conta através de mensagens de texto ou e-mails.

Não partilhe com ninguém nem divulgue o número do seu cartão de crédito ou a sua palavra-passe.

Utilize sempre uma rede Wi-Fi segura ao ligar-se ao site ou à aplicação móvel do seu banco. Nunca o faça a partir de uma rede Wi-Fi pública!

Se disponível, instale uma aplicação de segurança móvel que o alerte para qualquer atividade suspeita.

Verifique regularmente os seus extratos bancários.

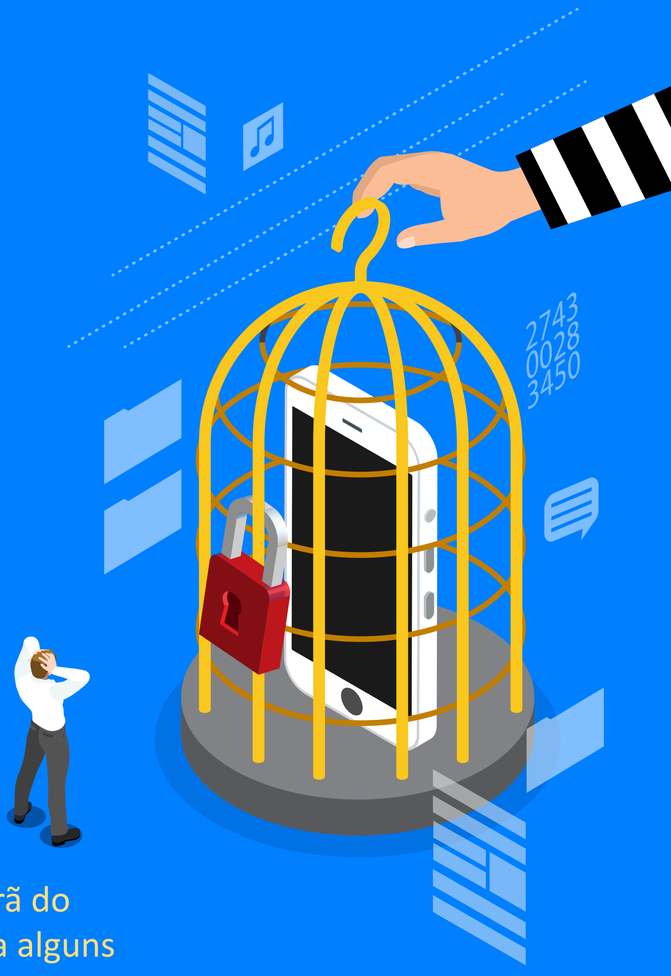
EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware

RANSOMWARE MÓVEL

DIGA ADEUS AOS SEUS FICHEIROS PESSOAIS



O ransomware retém o seu dispositivo móvel e os respetivos dados a um preço elevado. Este tipo de software malicioso bloqueia o ecrã do seu dispositivo ou impede o acesso a alguns ficheiros e funções.

COMO SE PROPAGA?

Ao visitar sites Web sujeitos a software malicioso.

Ao descarregar versões falsas de aplicações legítimas.

Ao clicar em hiperligações e anexos maliciosos integrados em e-mails de phishing.

QUAIS SÃO OS RISCOS?

Poderá ter de repor as definições de fábrica do dispositivo perdendo todos os seus dados.

Um invasor poderá ter livre acesso ao seu dispositivo e partilhar os seus dados com terceiros.

O QUE PODE FAZER?

Em intervalos regulares, faça uma cópia de segurança dos seus dados e mantenha todas as suas aplicações e o sistema operativo atualizados.

Evite adquirir produtos em lojas de aplicações de terceiros.

Se disponível, instale uma aplicação de segurança móvel que o alerte se o dispositivo estiver comprometido.

Evite e-mails e sites Web com ar suspeito ou que pareçam bons demais para ser verdade.

Não conceda direitos de administrador do dispositivo a ninguém.

Não pague o resgate. Estará a financiar criminosos e a encorajá-los a prosseguir com as atividades ilícitas.

EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware

AMEAÇAS DA WEB

OLHE DUAS VEZES ANTES DE CLICAR

Pode perder o seu dinheiro, a sua informação pessoal e até os dados armazenados, se o dispositivo parar de funcionar. Não se deixe apanhar!

COMO PODE ACONTECER?

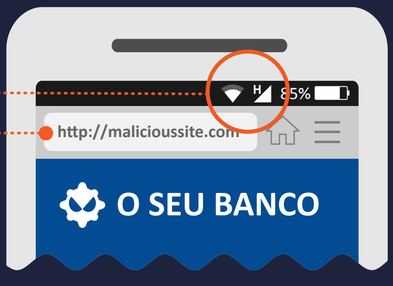
ATAQUES DE PHISHING: Enganam os utilizadores e levam-nos a fornecer informação pessoal fazendo-se passar por uma entidade credível. Propagam-se através do e-mail, mensagens de texto ou das redes sociais.

NAVEGAÇÃO EM SITES WEB: O seu dispositivo móvel pode ser infetado através de uma simples visita a um site Web não seguro.

TRANSFERÊNCIA DE FICHEIROS: As hiperligações e os anexos nocivos podem ser integrados diretamente num e-mail.

PORQUE É EFICAZ?

Os dispositivos móveis estão CONSTANTEMENTE LIGADOS à Internet.



O TAMANHO REDUZIDO DO ECRÃ DO DISPOSITIVO é uma condicionante geral. Os browsers dos dispositivos móveis mostram as URL num espaço de ecrã limitado, o que dificulta a confirmação da legitimidade do domínio.

A CONFIANÇA IMPLÍCITA DO UTILIZADOR na natureza pessoal de um dispositivo móvel.

O QUE PODE FAZER?

Desconfie de qualquer SMS ou chamada telefónica de uma empresa que solicite informação pessoal. Pode verificar se a mensagem/chamada é legítima ligando diretamente para o número oficial da empresa.

Ao navegar na Web através do seu dispositivo móvel, certifique-se de que a sua ligação é garantida através de HTTPS. Pode sempre confirmar olhando para o início da URL.

Nunca clique numa hiperligação/num anexo de um e-mail ou SMS não solicitado. Elimine-o imediatamente.

Tenha cuidado se este o conduzir para uma página com erros gramaticais, erros ortográficos ou de baixa resolução.

Se disponível, instale uma aplicação de segurança móvel que o alerte para qualquer atividade suspeita.

EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

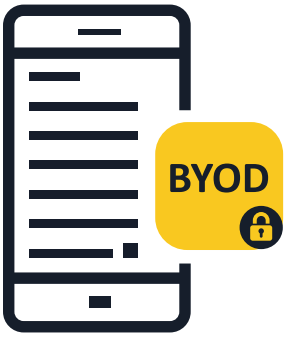
#MobileMalware

SOFTWARE MALICIOSO EM DISPOSITIVOS MÓVEIS

SUGESTÕES E CONSELHOS PARA EMPRESAS

1 Informe os seus colaboradores acerca dos riscos dos dispositivos móveis

- O trabalho com dispositivos móveis esbate as linhas que separam o uso profissional do uso pessoal. As empresas podem ser gravemente afetadas por um ataque que vise inicialmente o dispositivo móvel de um indivíduo. O dispositivo móvel é um computador e deve ser protegido como tal.



2 Implemente uma política empresarial BYOD (Bring-your-own-device, Traga o seu próprio dispositivo)

- Os colaboradores que utilizem os seus próprios dispositivos móveis para aceder a dados e sistemas da empresa (mesmo que se limitem a enviar e-mails, agendar compromissos ou aceder à base de dados de contactos) devem seguir as políticas da empresa. Escolha com cuidado as tecnologias a utilizar para gerir e proteger os dispositivos móveis, e incentive o pessoal a tomar as devidas precauções.

3 Inclua as políticas de segurança para dispositivos móveis no plano de segurança geral da empresa

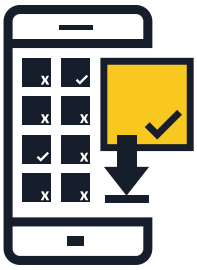
- Se um dispositivo não cumprir as políticas de segurança, não deverá permitir a respetiva ligação à rede da empresa nem o acesso aos dados corporativos. As empresas devem implementar as suas próprias soluções de Gestão de dispositivos móveis (MDM, Mobile Device Management) ou Gestão de mobilidade empresarial (EMM, Enterprise Mobility Management).
- Como complemento, é imperativo instalar uma solução de Defesa contra ameaças a dispositivos móveis (Mobile Threat Defence). Esta permitirá uma maior visibilidade e consciência contextual das ameaças a aplicações, redes e sistemas operativos.

4 Evite utilizar redes públicas de Wi-Fi para aceder aos dados da empresa

- Regra geral, as redes públicas de Wi-Fi não são seguras. Se um colaborador aceder aos dados da empresa utilizando uma ligação Wi-Fi gratuita de um aeroporto ou café, os dados podem ser expostos a utilizadores mal-intencionados. Aconselhamos as empresas a adotar e desenvolver políticas de "utilização eficaz" nesta matéria.

5 Mantenha os sistemas operativos e as aplicações dos dispositivos atualizados

- Aconselhe os seus colaboradores a descarregar as atualizações dos sistemas operativos dos respetivos dispositivos móveis sempre que tal for solicitado. Em especial, para quem utiliza o Android, pesquise os fornecedores de dispositivos móveis e fabricantes de telemóveis para conhecer as respetivas políticas de atualização. A instalação das atualizações mais recentes garante não só uma maior proteção do dispositivo, como também um melhor desempenho do mesmo.



6 Instale aplicações apenas de fontes seguras

- As empresas devem permitir apenas a instalação de aplicações de fontes oficiais nos dispositivos móveis ligados à rede utilizada pelas próprias empresas. Como opção, pondere criar uma loja de aplicações da empresa, através da qual os utilizadores finais podem aceder, descarregar e instalar aplicações autorizadas pela empresa. Consulte o seu fornecedor de segurança para obter informações de configuração ou defina as suas próprias configurações.

7 Evite o jailbreak

- 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. Não devem ser permitidos dispositivos com privilégios root no ambiente empresarial.

8 Pondere alternativas de armazenamento na nuvem

- É frequente os utilizadores de dispositivos móveis querem aceder a documentos importantes, não apenas através dos seus PC de trabalho, mas também a partir de telemóveis ou tablets particulares fora do escritório. As empresas devem avaliar a criação de um sistema de armazenamento seguro, baseado na nuvem, e de serviços de sincronização de ficheiros para satisfazer estas necessidades de forma segura.

9 Encoraje o seu pessoal a instalar uma aplicação de segurança móvel

- Todos os sistemas operativos correm o risco de serem infetados. Se estiver disponível, certifique-se de que os colaboradores utilizam 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.

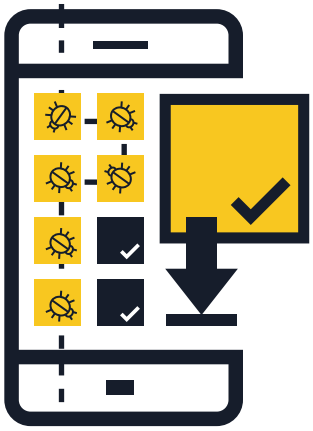
EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware

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.

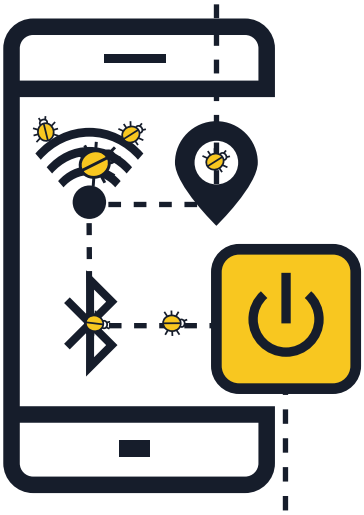
3 Termine a sessão nos sites Web depois de efetuar pagamentos

- **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.

EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware