FOLHA INFORMATIVA

# SEGURANÇA EM DISPOSITIVOS MÓVEIS

## O QUE É?

A disseminação da utilização das tecnologias de informação e comunicação (TIC) veio aumentar o volume de dados em circulação. As TIC têm-se tornado cada vez mais portáteis, sendo diversos os dispositivos móveis utilizados diariamente: em casa, no trabalho, na escola, na rua, entre outros, para aceder a notícias, para partilhar informação e para comunicar.

São vários os tipos de atividades criminais associadas ao uso de dispositivos móveis, entre os quais destacamos: infeção com *software* malicioso (vírus, etc.); furto de identidade; fraude em cartão de multibanco ou banco online; *hacking* a redes sociais ou e-mail; ciberataques que impedem o acesso a serviços públicos; material de abuso e de exploração sexual de crianças online; e-mails e telefonemas fraudulentos a solicitar dados pessoais; etc.

## QUEM É A VÍTIMA?

Qualquer pessoa pode ver a segurança dos seus dispositivos móveis comprometida, o que aumenta o risco de ser alvo de atividades criminais, como as anteriormente referidas.

## QUAL O IMPACTO?

Ser vítima de qualquer crime pode desencadear uma série de emoções, com as quais poderá ser difícil lidar.

Mesmo tratando-se de reações naturais perante um acontecimento inesperado, o processo para retomar o equilíbrio após a experiência de vitimação é gradual, variando de pessoa para pessoa. Todas as reações são possíveis, existindo formas muito diversificadas de lidar com a situação.

A pessoa que vê a segurança dos seus dispositivos comprometida e/ou que é alvo de um cibercrime na sequência desse comprometimento, pode sentir a sua privacidade e intimidade invadidas ou violadas. Como consequência, pode desenvolver sintomas de desconforto psicológico e emocional, incluindo problemas de sono, ansiedade e depressão.

**Se estas reações permanecerem ao longo do tempo, é importante a procura de apoio.**

## O QUE FAZER PARA DIMINUIR O RISCO?

**Bloqueio de ecrã** – Através da utilização de PIN, password, padrão desenhado, reconhecimento facial ou impressão digital, dificulta-se o acesso alheio a equipamentos/dispositivos móveis, protegendo, assim, o seu conteúdo, em caso de perda ou furto.

**Aplicações para localizar o smartphone e/ou apagar os conteúdos** – Existem diversas aplicações que permitem a localização do dispositivo e a eliminação dos seus dados à distância. O próprio Android e a Google disponibilizam nos equipamentos um sistema que possibilita a localização, a eliminação e o *reset* das definições.

**Instalação de aplicações de lojas oficiais** – Antes de descarregar uma aplicação, deverá ser verificada a sua origem e empresa responsável pela sua criação. Deve privilegiar-se o recurso a aplicações de lojas oficiais (ex.: Google Play, Apple Store), evitando-se a instalação de aplicações de fontes desconhecidas e/ou provenientes de hiperligações enviadas por e-mail e mensagens de texto.

**Utilização da *cloud*** – Permite guardar os conteúdos do dispositivo em segurança, podendo recuperá-los em outro equipamento.

**Identificação do IMEI** – Trata-se de um identificador do dispositivo que permite a deteção do/a seu dono/a. São 15 dígitos que surgem na embalagem original do equipamento, debaixo da bateria ou marcando *#06# seguido da tecla de chamada. Este código poderá ser solicitado, em caso de apresentação de queixa junto das autoridades.

**Informação à empresa de telecomunicações** – No caso de furto ou roubo do dispositivo móvel, deverá ser contactada a operadora, para anular o atual cartão e ser solicitada uma segunda via.

**Utilização de *software anti-malware*** e sua atualização regular.

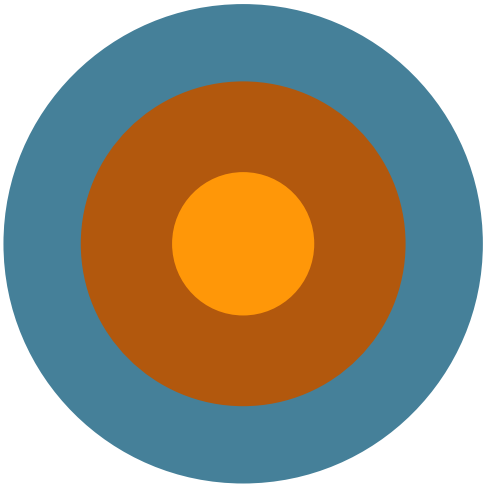
**Codificação do conteúdo do dispositivo** – Existem soluções no mercado que o fazem, através de um simples "guardar como", evitando assim que a informação seja utilizada por terceiros.

## QUE OUTRAS MEDIDAS DE SEGURANÇA SE PODEM ADOTAR?

- Evitar emprestar o dispositivo/equipamento ou partilhar as suas *passwords*.
- Manter o dispositivo no bolso ou na mala, quando não estiver a ser utilizado.
- Evitar expor o dispositivo à vista de terceiros ou sem supervisão.
- Utilizar ou transportar o dispositivo com discrição, evitando atrair a atenção para a sua existência.

### DADOS ESTATÍSTICOS

Segundo dados do Relatório *Cibersegurança em Portugal*, do Centro Nacional de Cibersegurança, referente a 2018, verificou-se que poucos indivíduos (cerca de 3%) se sentem muito bem informados quanto ao risco de cibercrime.



- **37%** dos/as portugueses/as utilizam a mesma *password* das redes sociais para *login* em outros serviços
- Apenas **24%** dos/as portugueses/as usam um sistema de segurança no *smartphone*
- Apenas **11%** das famílias discutem o risco online com os/as filhos/as

FONTE: *Relatório Cibersegurança em Portugal (2019)*. Disponível em https://www.cncs.gov.pt/content/files/relatrio_sociedade_2019_-_observatrio_de_cibersegurana_cncs_v3.pdf

## QUE APOIO ESTÁ DISPONÍVEL?

Em caso de crime contra dispositivos móveis, a queixa ou denúncia pode ser apresentada junto de uma das seguintes autoridades:

- Ministério Público;
- Polícia Judiciária;
- Polícia de Segurança Pública;
- Guarda Nacional Republicana.

A APAV está também disponível para apoiar. O apoio é gratuito e confidencial. Poderá contactar a APAV:

- Pela Linha de Apoio à Vítima - 116 006 | chamada gratuita | dias úteis das 09h às 21h;
- Pela Linha Internet Segura - 800 21 90 90 | linhainternetsegura@apav.pt | dias úteis das 09h às 21h;
- Através de qualquer Gabinete de Apoio à Vítima da APAV (contactos em https://apav.pt/apav_v3/index.php/pt/contactos).

**RECURSOS APAV**
www.apav.pt/cibercrime/
www.infovitimas.pt
www.apav.pt/folhasinformativas

**OUTROS RECURSOS**
https://www.cncs.gov.pt