APAV
associação portuguesa de Apoio à Vítima

25 ANOS
A dar voz ao silêncio

# Folha Informativa

## SEGURANÇA DISPOSITIVOS MÓVEIS

### O QUE É?

Existem milhões de telemóveis, smartphones e tablets em Portugal, com equipamentos a serem roubados ou perdidos constantemente, na maior parte em bares ou noutras superfícies comercias. No entanto, a maioria dos roubos ocorrem devido a máfias organizadas especializadas no método de 'alunizage', o que faz com que a perda deste dispositivo não seja apenas um transtorno, mas também um grande risco devido à quantidade de informação que o mesmo armazena, tanto a nível pessoal como profissional. Este processo utiliza a clonagem de informação do dispositivo passando-a para outro.

### QUEM É A VÍTIMA?

Qualquer pessoa pode ser vítima deste tipo de crime.

### QUAL O IMPACTO?

Ser vítima de um crime pode desencadear uma série de reações emocionais. Pode vivenciar uma combinação de emoções e pensamentos com os quais é por vezes difícil lidar. Mesmo que estas emoções sejam reações completamente normais, pode sentir que está quase a ir abaixo e a perder o controlo, o que pode ser bastante assustador. É importante lembrar que, na maioria das situações, isto passará e que, com o tempo, irá gradualmente voltar a adquirir um sentimento de controlo sobre a sua vida. Das reações aqui descritas, pode identificar-se com muitas delas mas também pode não reconhecer nenhuma. O importante é perceber que não existe uma forma pré-definida de como pode reagir.

Quando somos vítimas de um crime, podemos ser afetados de muitas maneiras diferentes. Todos nós temos as nossas estratégias para lidar com as dificuldades na nossa vida. Habitualmente, estas estratégias funcionam bastante bem e ajudam-nos em circunstâncias muito diferentes. Mas quando se é vítima de crime somos colocados numa situação à qual reagimos de modo diferente do habitual e as estratégias que normalmente usamos poderão não ser suficientes.

Frequentemente sentimos que a nossa integridade pessoal foi violada e que estamos em estado de choque. Para além disso, podemos sofrer de problemas como dificuldades em dormir, depressão, ansiedade e culpa. Podemos sentir culpa, mesmo sabendo que na verdade não somos culpados pelo que aconteceu. Para a maioria das pessoas, estes sintomas desaparecem com o tempo. **Se estas reações não desaparecem passados alguns meses, é importante procurar ajuda.**

Que se pode fazer para diminuir o risco?

- **Bloqueio do ecrã** – No caso de perda ou roubo, esta é uma boa medida para salvaguardar os dados e evitar o uso imediato e indiscriminado de quem se quer aproveitar desta situação. É possível configurar esta funcionalidade para que se ative no momento em que desliga o ecrã, impedindo o acesso ao equipamento sem uma password ou um PIN. Variando de dispositivo para dispositivo, é possível escolher entre cinco bloqueios: PIN, password, padrão desenhado na tela, reconhecimento facial e leitor de impressão digital.

- **Bloqueio do SIM** – Bloquear o cartão SIM com um PIN de quarto números impede que seja possível ser usado noutro telefone, evitando prováveis sustos na factura e também que que se possa anular o bloqueio do ecrã com um "hard reset" (processo em que se coloca o telefone nas configurações de fábrica), sempre que o combinado com uma password do ecrã.

- **Aplicações para localizar o smartphone e/ou apagar os conteúdos** – Existem várias aplicações, que permitem localizar um dispositivo ou apagar os seus dados à distância. Mesmo assim, o próprio Android e a Google oferecem em todos os dispositivos um sistema menos sofisticado mas que permite a localização do dispositivo num mapa, a eliminação dos dados ou o reset das definições de fábrica à distância.

- **A Cloud como cópia de segurança** – todos os dispositivos têm a possibilidade de armazenar a informação na Cloud. Pode proteger

tudo caso perca o equipamento, de forma a depois recuperar tudo imediatamente utilizando outro equipamento com a mesma conta. Esta prática é sempre recomendada quando a informação armazenada na cloud não é sensível. Caso se trate de informação profissional deverá ter em conta as políticas da empresa.

- **Saber o IMEI** – é uma medida recomendável para qualquer telefone móvel. Trata-se de um número com 15 dígitos que identifica cada um dos dispositivos existentes e que será solicitado pela polícia caso denunciar um roubo. Embora seja pouco provável a recuperação do dispositivo, serve para confirmar o dono desse equipamento. O número normalmente vem na embalagem original do telefone, mas também se pode encontrá-lo debaixo da bateria ou clicando na sequência *#06# e tecla de chamada de qualquer terminal.

- **Passwords para limitar o acesso às aplicações** – algumas aplicações oferecem a possibilidade de ter um maior nível de segurança, permitindo configurar um acesso com password. É também possível utilizar aplicações que se encarregam de esconder o conteúdo que queremos manter a salvo dos intrusos.

- **Evite emprestar o equipamento ou partilhar as passwords** – Não é estranho ver empréstimos de telemóveis, sobretudo entre os mais jovens, que chegam a partilhar, em nome de uma boa amizade, as senhas para aceder aos espaços privados do seu telemóvel, o que é algo a evitar a todo o custo. Se não tem outra solução além do empréstimo do telemóvel, deverá sempre fazer empréstimos por pouco tempo, e sob a sua supervisão. Deverá depois trocar as passwords.

- **Codificar o conteúdo do dispositivo** – Uma das melhores opções para evitar que a informação do dispositivo seja utilizada por terceiros é codificá-la. Existem soluções no mercado que fazem isto de uma forma simples e sistemática, com um simples 'Guardar como".

- **Avisar a empresa de telecomunicações** – As zonas movimentadas são os espaços preferidos pelos profissionais dos assaltos. Se for vítima de roubo, deve ligar o quanto antes para a sua operadora ou visitar uma das suas lojas para anular o cartão e pedir uma segunda via.

- **Use um software anti-malware** Deve usar sempre um software anti-malware de forma preventiva e com uma instalação atualizada.

## DADOS ESTATÍSTICOS

Em apenas um ano os ciberataques aos telemóveis aumentaram mais de 600%. Entre março de 2012 e março de 2013, o número de programas perniciosos introduzidos sub-repticiamente nos telefones com acesso à internet aumentou 614 %, calculou a empresa Juniper, situada em Silicon Valley, na Califórnia.

TESTEMUNHO

Achei sempre que utilizar o smartphone era uma coisa que não tinha riscos. Tinha por hábito fazer algumas compras por internet e tinha as passwords todas marcadas como visíveis. Quando perdi o smartphone, alguém utilizou esses acessos e fez um grande desfalque na minha conta bancária. Apesar de ter informado a operadora e o banco e ter cancelado contas, durante muito tempo continuei com este problema. Para além disso, também tiveram acesso a informação privada, como e-mails e contatos, que me gerou grande ansiedade durante um longo período de tempo.

**Recursos**

A queixa ou denúncia pode ser apresentada junto de uma das seguintes autoridades:

Ministério Público (MP)
Polícia Judiciária (PJ)
Polícia de Segurança Pública (PSP)
Guarda Nacional Republicana (GNR)

Qualquer uma destas autoridades tem o dever de receber todas as queixas e denúncias que lhe sejam apresentadas, mesmo que o crime não tenha sido cometido na respetiva área territorial ou, no caso das polícias, a investigação não seja da sua competência.

infovitimas.pt

complique.org

apav.pt/folhainformativa

APAV 2015
apav.sede@apav.pt

donativos
NIB 0036 0000 99105881577 83

CHAMADA GRATUITA
116 006
LINHA DE APOIO À VÍTIMA
DIAS ÚTEIS DAS 09H-19H

APAV
associação portuguesa de Apoio à Vítima

facebook.com/apav.portugal
apav.pt
infovitimas.pt

parceria

Procuradoria-Geral da República