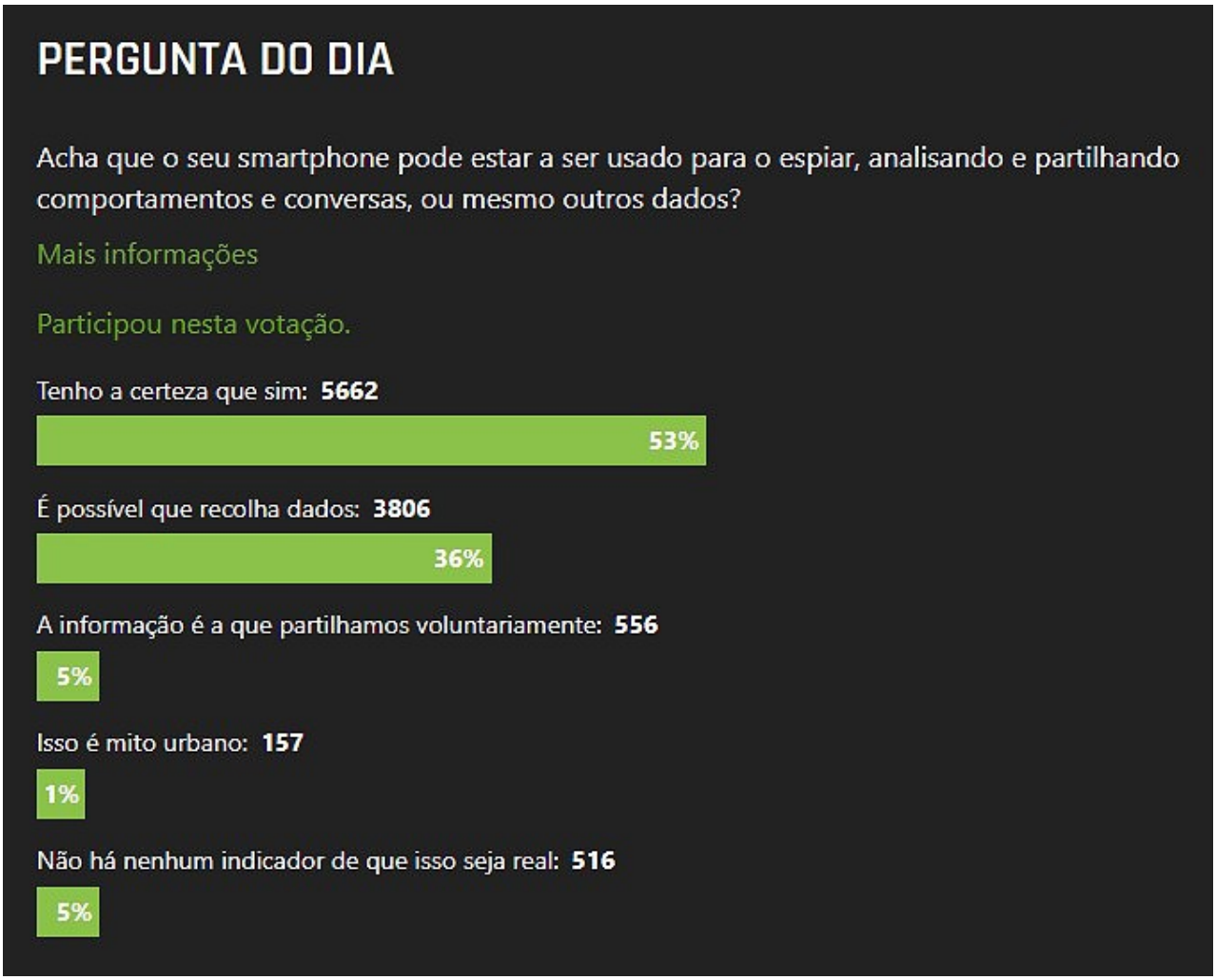
53% acreditam que smartphones podem ser usados para nos espiar. O que dizem os especialistas?

tek.sapo.pt/noticias/internet/artigos/53-acreditam-que-smartphones-podem-ser-usados-para-nos-espiar-o-que-dizem-os-especialistas

Francisca Andrade 21 de julho de 2023

Será que os nossos smartphones podem estar a ser usados para nos espiar, analisando e partilhando comportamentos e conversas, ou mesmo outros dados? **Para a maioria dos leitores que participaram na mais recente sondagem do SAPO TEK esta é uma certeza.**

Ao todo, na nossa votação, recebemos 10.266 participações. **Deste conjunto, 53% dos leitores (5.427) votaram na opção "Tenho a certeza que sim"**. Já 36% (3.800) acreditam que é possível que os smartphones estejam a recolher dados desta forma.



Resultados da sondagem lançada pelo SAPO TEK.

Por outro lado, para **5% dos leitores que participaram na sondagem (556), "a informação é a que partilhamos voluntariamente**". Outros 5% (515) acreditam que não existe qualquer indicador de que esta situação seja real e **1% (156) defendem que a mesma não passa de um mito urbano**.

Mas, os nossos smartphones estão mesmo a espiar-nos? **O SAPO TEK falou com especialistas da área da cibersegurança, assim como dos direitos digitais, para esclarecer esta questão.**

"A nossa privacidade é um efeito colateral"

Para lá dos casos de spyware, onde os smartphones são infectados com software malicioso que dá aos cibercriminosos a possibilidade de terem acesso privilegiado a dados presentes nos equipamentos, **há quem também quem considere que os processos de recolha e gestão de informação feitos pelas empresas tecnológicas**, entre fabricantes de smartphones e criadoras de aplicações, **se podem constituir como uma espécie de "espionagem"**.

Ao SAPO TEK, **Ricardo Lafuente, vice presidente da Associação D3 - Defesa dos Direitos Digitais**, admite que a ideia de estarmos rodeados de aparelhos que nos estão a espiar a cada movimento é algo do campo da ficção científica, **no entanto, categorizá-**

la como mito urbano não é totalmente correto.

O responsável dá o exemplo das smart TVs, indicando que está documentado que existem marcas que **"estão a fazer uma recolha ativa do que estamos a ver e isso faz parte do modelo de negócio"**.

"A recolha de dados é uma forma de subsidiar", explica. "Se formos a reparar, comparando com o que eram há 10 anos, não é pelos materiais diferentes que [as smart TVs] são agora mais baratas: é através da recolha de informação ativa, e está documentado, várias marcas fazem *screenshots* regulares do que estamos a ver na nossa TV, algumas até gravam áudio para ser transmitido à empresa e para depois ser então valorizado segundo os seus termos".

> "Obviamente, à luz do RGPD, da doutrina de dados europeia, é um pesadelo que ainda está por explorar, sobretudo porque as comissões nacionais de dados não têm os meios para estarem a fazer revisões compreensivas de toda a tecnologia que nos rodeia", afirma Ricardo Lafuente.

Como realça o responsável, **"o incentivo para a recolha maximal de dados é demasiado grande para as empresas não o aproveitarem"**. Esta é, no entanto, uma situação que acarreta um vasto conjunto de problemas para a privacidade dos utilizadores.

Olhando para o caso específico das aplicações para smartphones, Ricardo Lafuente lembra os recentes casos de polémicas relacionadas com a partilha de dados por parte de empresas responsáveis por apps de gestão do ciclo menstrual.

Ainda em maio deste ano, a organização Ius Omnibus acusou a Flo Health, empresa responsável pela Flo, uma app de gestão do ciclo menstrual, de partilhar com terceiros, e para fins comerciais, dados de utilizadoras portuguesas sem o seu consentimento.

Além de alertar para a possibilidade de fugas de dados nos casos onde a informação é armazenada e agregada de forma irresponsável, o vice presidente da Associação D3 enfatiza que, **com este tipo de práticas, "passam a existir bases de dados com esta informação toda e, mesmo que a empresa não faça nada, é muito problemático"**, sobretudo quando se trata de **"dados de uma intimidade absolutamente aterradora de ser explorada, até comercialmente, porque é, de facto, o que acontece"**.

"Acho que o termo espionagem concentra a preocupação nesta ideia de que as agências do governo nos estão a espiar, quando, na verdade, **é uma recolha indiscriminada de dados com a esperança de os conseguir usar para os vender ou para os rentabilizar de alguma forma e a nossa privacidade é um efeito colateral desse modelo de negócio**", defende o responsável.

Realçando que "existe razão para alarme quanto à recolha de dados", Ricardo Lafuente acrescenta ainda que **"a simples existência deste paradigma de recolha integral é algo que a União Europeia tem vindo a questionar e a querer estancar, mas ainda**

não estamos lá”.

Spyware também o pode afetar: o que fazer?

O spyware não é apenas algo que afeta, por exemplo, altas instâncias de entidades governamentais. **Para os cibercriminosos, os dados são valiosos e, na dark web, o preço da nossa informação pessoal pode ir até aos milhares de dólares**. Em muitos dos casos, o “software espião” surge em aplicações, que, à vista desarmada, até podem parecer legítimas.

Ao SAPO TEK, **fonte oficial do Centro Nacional de Cibersegurança** (CNCS), afirma que “o smartphone tornou-se num objeto essencial para aceder à Internet, não é apenas um telemóvel, mas um autêntico computador de bolso onde se encontram múltiplas funcionalidades”.

“Esta importância nem sempre é acompanhada pela correspondente preocupação com a cibersegurança”, realça o CNCS, lembrando que **“é preciso ter algum cuidado com os critérios que são utilizados” para instalar novas aplicações** e “com as autorizações de acesso a funcionalidades que são atribuídas”.

“As aplicações disponibilizadas fora das plataformas reconhecidas para o efeito são menos sujeitas a verificação e crítica”, motivo pelo qual **“é mais provável encontrar uma aplicação maliciosa nesse contexto, a qual pode trazer consigo software que, por exemplo, espie os utilizadores e viole os seus dados pessoais”**, sublinha a entidade.

Em linha com o CNCS, também **Miguel López Negrete, Head of Threat Intelligence da S21sec Cyber Solutions by Thales**, e **Bruno Castro, fundador e CEO da VisionWare**, alertam para os riscos de cibersegurança que existem.

“Existem várias formas de malware capazes de espiar os utilizadores de dispositivos móveis, sobretudo em sistemas operativos Android, mas também em iOS”, afirma Miguel López Negrete. **“Em casos mais avançados, o software malicioso pode ser praticamente indetetável pelo utilizador visado”**.

Já Bruno Castro salienta que **“um dos principais erros que as pessoas cometem quando utilizam uma aplicação é presumir que esta, simplesmente por estar disponível, é completamente segura”**.

Nas palavras do fundador e CEO da VisionWare, “**o WhatsApp é uma das plataformas mais vulneráveis a esta presunção**, já que muitos dos seus utilizadores acreditam que o sistema de mensagens encriptadas é inviolável e só os intervenientes é que têm acesso às mesmas”.

> “Além de poder ser alvo de casos de hacking, com especialistas informáticos a conseguir quebrar facilmente o código de encriptação do serviço, os metadados destas mensagens podem ser igualmente vulneráveis a intrusão ou a vigilância por parte de terceiros capazes de o fazer”, afirma o responsável.

Bruno Castro aponta também que é preciso ter **“atenção redobrada no que se refere aos links, em particular, nos grupos de Whatsapp”**. “Muitas vezes, estes links executam pequenos pedaços de código no nosso smartphone, os quais podem implicar sérios problemas de invasão e roubo de dados confidenciais”.

Embora a comunicação de voz no WhatsApp seja encriptada, o responsável detalha, no entanto, que **“a estrutura que suporta a aplicação guarda toda a sua informação e essa infraestrutura, por sua vez, não é infalível”**.

Mas o que fazer para não ser alvo de aplicações de spyware? O CNCS deixa um conjunto de recomendações importantes para os utilizadores.

- **Seja cuidadoso com as aplicações que instala**, optando por apps que são disponibilizadas por plataformas reconhecidas. É também importante que verifique as avaliações de utilizadores e especialistas e que limite o acesso das aplicações apenas às funcionalidades essenciais ao seu funcionamento;
- **Restrinja ao máximo as configurações de segurança e privacidade do seu smartphone e aplicações**
- **Mantenha o sistema e as aplicações atualizados**
- **Utilize uma rede virtual privada (VPN) sempre que se ligar a uma rede Wi-Fi pública** ou então opte por utilizar os dados para aceder à Internet em lugares sem Wi-Fi doméstico ou profissional
- **Evite ter o Bluetooth e a localização do seu smartphone ligados desnecessariamente**
- **Não clique em links enviados através de SMS suspeitos**, o mesmo se aplica às ligações suspeitas que surgem em mensagens que recebe através de outras plataformas de comunicação.

Aproveite também para recordar, na galeria que se segue, **sete hábitos para reforçar a segurança e fazer face às ameaças do mundo online.**

Clique nas imagens para ver com mais detalhe

- 

- 
Login
Password
- 
- 
DOWNLOAD
- 
- 
-