Temu tem “uma aplicação irmã” que foi suspensa pela Google por suspeitas de ser software malicioso

expresso.pt/geracao-e/2023-10-20-Temu-tem-uma-aplicacao-irma-que-foi-suspensa-pela-Google-por-suspeitas-de-ser-software-malicioso-ccca66ea

A *Temu*, que atualmente está em primeiro lugar na *Playstore* e na *Appstore*, é uma aplicação de *marketplace* (mercado online que vende produtos de terceiros) que tem como dona a PDD Holdings Inc. Esta é a mesma empresa que detém a aplicação *Pinduoduo,* uma aplicação que foi suspensa pela Google, em março deste ano, por ser alvo de suspeitas de se tratar de *malware*.

Segundo a CNN, o *malware* (que significa *software* malicioso) era **capaz de contornar a segurança do telemóvel dos utilizadores para monitorizar atividades noutras aplicações, verificar notificações, ler mensagens privadas e alterar definições**. Mas será que devemos estar **preocupados com a aplicação *Temu***? O presidente executivo (CEO) da VisionWare, Bruno Castro, considera que sim. “Diria que devemos ficar bastante preocupados com esta aplicação”, diz.

Bruno Castro reforça que “esta e outras aplicações chinesas recorrem a práticas de privacidade e de proteção de dados pessoais contrárias às utilizadas no Ocidente, e de forma obscura”, mas, neste caso, a “preocupação ganha ainda maior relevância”. Afinal de contas, a “aplicação irmã, a *Pinduoduo*, foi suspensa pela Google por suspeitas de malware”. O CEO da VisionWare realça que “pode existir um potencial acesso de Pequim aos dados dos utilizadores”.

“Algo curioso é o facto de, apesar de ter sido dissolvida, a equipa de engenheiros da *Pinduoduo* ter sido transferida na sua totalidade para a *Temu*. Este dado lança a questão: que garantias existem de que a *Temu*, composta pelos mesmos elementos, não estará também a agir da mesma forma?”, afirma Bruno Castro.

Se dúvidas existem sobre os dados que a *Temu* pode estar a recolher, o melhor é dar uma leitura pelas políticas de privacidade da aplicação antes de se registar. No ponto “Recolha automática de dados” pode ler-se que a aplicação recolhe:

- Dados do dispositivo, “como o tipo e a versão do sistema operativo do seu computador ou dispositivo móvel, fabricante e modelo, tipo de navegador, resolução do ecrã, tamanho da RAM e do disco, utilização da CPU, tipo de dispositivo (...) informações gerais de localização, como cidade, estado ou área geográfica”;
- Dados de atividade online, “tais como páginas ou ecrãs que visualizou, quanto tempo passou numa página ou ecrã, o website que visitou antes de navegar para o Serviço, caminhos de navegação entre páginas ou ecrãs, informações sobre a sua atividade numa página ou ecrã, tempos de acesso e duração do acesso”;

- Dados de localização, “incluindo os seus dados de localização gerais (...) e os dados de localização exatos do seu dispositivo móvel”.

Henrique Santos, professor da Escola de Engenheira da Universidade do Minho, sublinha que **“a larga maioria das aplicações têm um modelo de negócio escondido, relacionado com a informação que conseguem capturar do utilizador”**. É importante perceber que a informação recolhida “não é apenas a informação pessoal que inserimos", mas também a comportamental. “No caso da aplicação *Temu*, acresce que ela é de origem chinesa e **os valores promovidos pela sociedade chinesa são diferentes dos nossos**. Há operações no negócio que nós entendemos terem limites éticos e que para a sociedade chinesa (bem como para outras) não o são.”

Mas afinal que preocupações devemos ter enquanto internautas?

“Devemos manter-nos **muito atentos, preventivos e, sobretudo, não clicar em links cujas origens não conhecemos** ou poderão ser de índole duvidosa e/ou criminosa. Por norma, devemos desconfiar, sempre”, reforça Bruno.

Quando instalamos aplicações nos nossos telemóveis ou *tablets*, devemos t**er em atenção as permissões que concedemos às aplicações**. “Muitos destes serviços ganham dinheiro a vender os seus dados e, para isso, requisitam acesso à sua localização, ao seu microfone e à sua câmara. Há que verificar, com muita atenção, as definições do seu telemóvel e controlar as permissões que dá a cada uma delas”.

O presidente executivo da VisionWare reforça que há **“medidas de “higiene” cibernética”, entre as quais, utilizar *passwords* fortes e com autenticação em, pelo menos, duas etapas**. Além disso, a atenção nunca é em demasia quando se fala da Internet, de aplicações e de redes sociais. “Ainda que seja uma pessoa conhecida, muito próxima ou um familiar, valide sempre primeiro com o próprio visado, antes de responder a qualquer situação, ou pior, antes de partilhar qualquer informação pessoal, antes que seja tarde demais”.

Mas se, ainda assim, quiser “comprar como um milionário?”

A *Temu* ficou especialmente conhecida depois de ter emitido o seu anúncio na Super Bowl com o lema “compre como um milionário”. A verdade é que a aplicação apresenta preços competitivos e, por isso, gera a tentação de arriscar e de a utilizar. O professor da Universidade do Minho apresenta um **guia para aqueles que estão “predispostos a trocar alguma privacidade por um desconto”**:

1. Criar um e-mail novo, sem atividade pessoal ou profissional, só para efeitos de registo nesta app (ou outras semelhantes). Nunca fazer o upload de uma foto real e dar o mínimo de informação possível;

2. Utilizar, se possível, uma VPN de confiança, o que permitirá esconder a verdadeira localização;
3. Quando aceder ao site usar um browser diferente do que é utilizado habitualmente; assim, a eventual exposição de informação fica limitada;
4. Usar um cartão temporário de uma utilização apenas. Nunca fornecer detalhes de qualquer conta bancária ou mesmo do PayPal;
5. Limpar a cache do browser depois da utilização o que limita a capacidade de, remotamente, a empresa explorar o que quer que tenha sido carregado para o equipamento local;
6. Limitar as autorizações da App, sempre que possível; na maioria dos casos isso impede que elas funcionem, mas se claramente a App está a solicitar autorizações de acesso que não se justificam, então a intenção não é boa, naturalmente.

E se suspeitar que o meu dispositivo tem algum *malware*?

A solução pode "variar dependendo da gravidade do problema". Segundo Bruno Castro, **"a forma mais eficiente seria a de formatar o dispositivo móvel"**. Contudo, o especialista recomenda que "em primeiro lugar se desinstale a aplicação e se reinicie o dispositivo". Depois disso, é importante verificar que "o sistema operativo é o mais recente". Além disso, é fundamental "rever as permissões que foram concedidas à aplicação" e "alterar as palavras-passe para evitar acessos indesejados".

Além disso, Henrique Santos lembra que "os fabricantes fornecem algum tipo de suporte para avaliar a segurança dos dispositivos e alertar para potenciais problemas".