As empresas de telecomunicações dos EUA, incluindo AT&T, Verizon e Lumen, têm sido alvo de ataques de espionagem massivos e aparentemente sofisticados há vários meses. A China é o principal suspeito por trás dos hacks. Como resultado, as autoridades estão aconselhando o público em geral a usar aplicativos criptografados para suas mensagens e chamadas, para evitar que hackers possam acessar suas comunicações.

O uso de aplicativos não criptografados, como SMS normais, sempre representa o risco de interceptação por uma parte nefasta que obtém acesso à rede de telecomunicações. Neste caso, os clientes da AT&T e da Verizon correm o risco de ter as suas comunicações espionadas.

Felizmente, na era dos smartphones, existem muitos aplicativos criptografados de ponta a ponta para mensagens e chamadas. A criptografia ponta a ponta refere-se ao tipo de segurança forte que os hackers não podem violar. E a melhor parte é que você já pode ter aplicativos criptografados no seu iPhone e dispositivo Android sem saber.

Seja qual for o caso, as soluções a seguir podem ajudar até que as autoridades digam que os hackers foram frustrados para sempre.

O que você vai ler:

Tecnologia. Entretenimento. Ciência. Sua caixa de entrada.

Inscreva-se para receber as notícias mais interessantes sobre tecnologia e entretenimento.

Ao me inscrever, concordo com os Termos de Uso e li o Aviso de Privacidade.

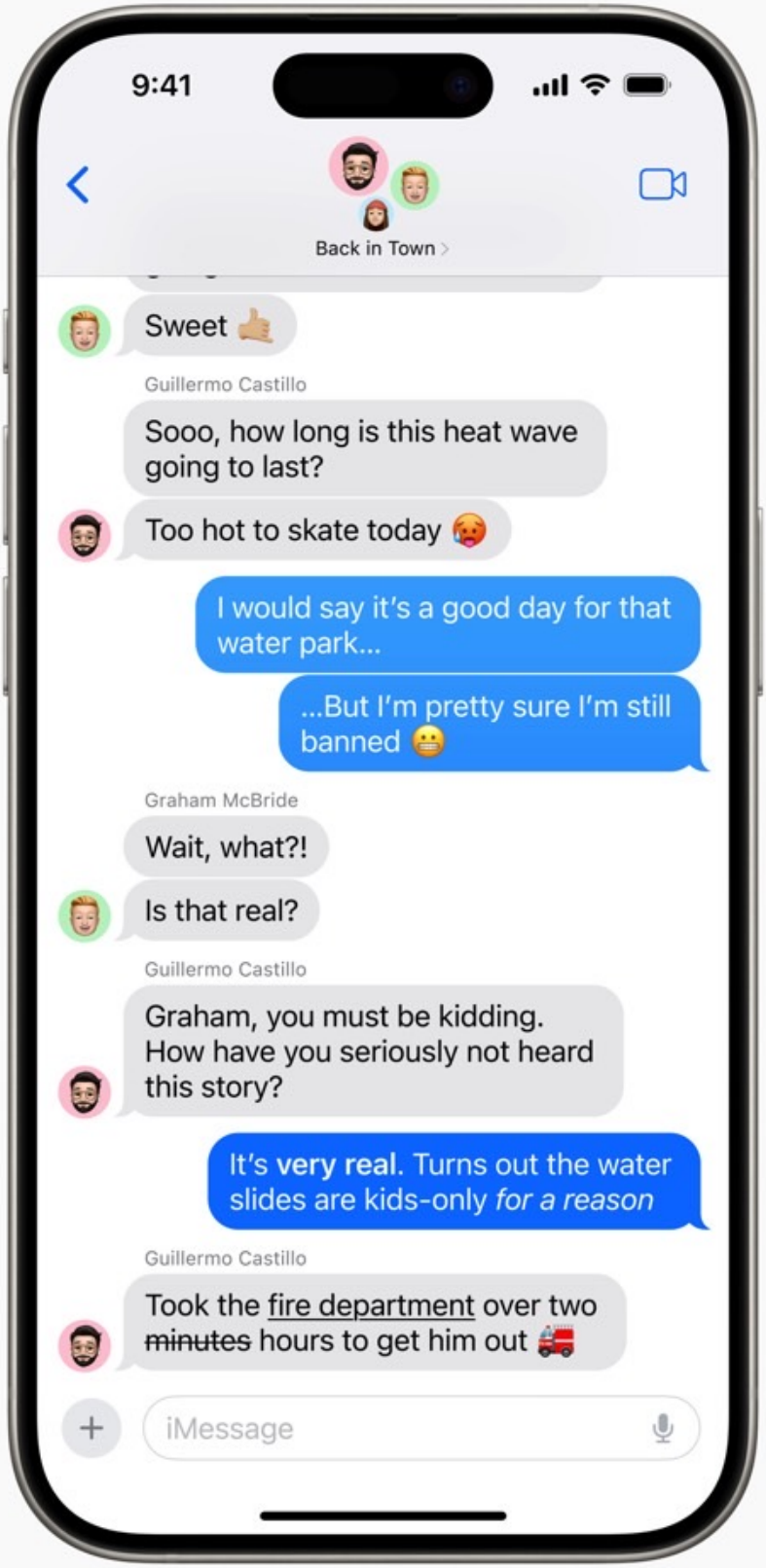
De acordo com *Notícias da NBC*as autoridades de segurança recomendam o uso de aplicativos de mensagens criptografadas para evitar que a China possa interceptar suas comunicações.

“Nossa sugestão, o que dissemos às pessoas internamente, não é nova aqui: a criptografia é sua amiga, seja em mensagens de texto ou se você tiver a capacidade de usar comunicação de voz criptografada. Mesmo que o adversário consiga interceptar os dados, se estiverem criptografados, isso tornará isso impossível”, disse Jeff Greene, diretor-assistente executivo de segurança cibernética da Agência de Segurança Cibernética e de Infraestrutura.

“As pessoas que buscam proteger ainda mais as comunicações de seus dispositivos móveis se beneficiariam ao considerar o uso de um celular que receba automaticamente atualizações oportunas do sistema operacional, criptografia gerenciada de forma responsável e resistente a phishing”, acrescentou um funcionário não identificado do FBI.

Greene observou ainda que é impossível “prever um prazo para o despejo total”. Talvez você precise se acostumar a confiar em aplicativos criptografados para mensagens e chamadas por um bom tempo.

iMessage


9:41
Back in Town
Sweet
Guillermo Castillo
Sooo, how long is this heat wave going to last?
Too hot to skate today
I would say it's a good day for that water park...
...But I'm pretty sure I'm still banned
Graham McBride
Wait, what?!
Is that real?
Guillermo Castillo
Graham, you must be kidding. How have you seriously not heard this story?
It's very real. Turns out the water slides are kids-only for a reason
Guillermo Castillo
Took the fire department over two minutes hours to get him out
iMessage

F

onte da imagem: Apple Inc.

O aplicativo de mensagens padrão do iPhone tem sido o aplicativo de mensagens de texto padrão que os rivais tentam replicar e superar há anos. A Apple também estabeleceu um padrão de alta segurança com a criptografia ponta a ponta do iMessage. Este é o aplicativo que você deve usar para garantir que todos os seus bate-papos estejam protegidos.

A desvantagem é que a criptografia ponta a ponta se aplica apenas às suas “bolhas azuis”. Estas são as iMessages criptografadas. Se você vir bolhas verdes no seu iPhone, evite-as, pois são textos SMS ou RCS.

Do que você precisa: iPhone, iPad ou Mac e conexão com a internet.

FaceTime

FaceTime é o equivalente do iMessage da Apple, mas para chamadas de voz e vídeo. É criptografado e você pode alternar facilmente entre chamadas de voz e vídeo com um toque rápido.

Do que você precisa: iPhone, iPad ou Mac e conexão com a internet.

Sinal

Signal é um aplicativo de terceiros disponível para iPhone e Android. Ele suporta criptografia ponta a ponta como iMessage e FaceTime e pode ser o aplicativo perfeito para comunicação entre plataformas.

O Signal vem com suporte para mensagens e chamadas, então você não precisa de dois aplicativos separados.

Embora você possa usá-lo para se comunicar com usuários de iPhone e Android, o Signal deve ser instalado separadamente.

Do que você precisa: iPhone ou Android e conexão com a internet.

WhatsApp

Fonte da imagem: José Adorno para BGR

O WhatsApp é o aplicativo de bate-papo mais popular do mundo, pertencente ao império de redes sociais da Meta. O WhatsApp tinha suporte para criptografia de ponta a ponta antes do Meta (então Facebook) comprá-lo, e o Meta manteve o recurso em vigor desde então.

Assim como o Signal, é um aplicativo de terceiros que você precisa instalar no seu dispositivo, mas funciona tanto com dispositivos iPhone quanto com Android.

Também como o Signal, você obtém suporte para mensagens de texto e chamadas criptografadas, tudo em um único aplicativo.

Do que você precisa: iPhone ou Android e conexão com a internet.

Mensagens do Google – com uma grande advertência de segurança

Também adicionarei o aplicativo Mensagens do Google no Android como uma solução potencialmente segura e criptografada para mensagens de texto, mas com uma grande ressalva. O Google usa o padrão RCS, que não é criptografado de ponta a ponta. Apenas a versão do RCS do Google oferece criptografia de ponta a ponta. Não está disponível em todos os dispositivos Android e não está disponível em iPhones.

Portanto, se você usar o Mensagens do Google para criptografar seus bate-papos, terá que garantir que a outra pessoa na cadeia de texto também use as mensagens RCS do Google com suporte para criptografia.

O que você precisa: Android com RCS do Google Messages ativado e conexão à Internet.

Mais uma coisa

Pode haver outros aplicativos criptografados de bate-papo e chamadas ou aplicativos que afirmam oferecer esse tipo de segurança. Os acima são os mais populares e conhecidos por sua segurança (com a exceção do Google RCS acima). Certifique-se de fazer sua lição de casa ao escolher aplicativos para iPhone ou Android menos conhecidos ou parcialmente criptografados.

Eu sempre disse que os hacks catastróficos da AT&T e da Verizon provam que a Apple estava certa sobre a criptografia do iPhone. A insistência da Apple em proteger seus produtos forçou outros a seguirem o exemplo.

Quer o ataque da China que durou meses seja resolvido em breve ou demore um pouco para ser totalmente corrigido, você deve se acostumar a usar aplicativos de comunicação criptografados. Não se trata de esconder o que você faz; trata-se do princípio de proteger sua privacidade.

Também observarei que as agências de aplicação da lei não são tão rápidas em recomendar criptografia quanto em pedir a empresas como a Apple que criem backdoors. Como mostra este ataque, os hackers encontrarão pontos de entrada que serão explorados, portanto a criptografia é sempre a melhor aposta.