Latest WhatsApp hack highlights dangers of using consumer-grade (free) apps for business

Businesses using Consumer Apps risk facing stiff regulatory fines for data loss or worse

LONDON, UK, May 14, 2019 /EINPresswire.com/ --
Armour Communications, the leading provider of specialist, secure communications solutions, calls for organisations to stop using consumer-grade, free apps when handling sensitive or commercial information. For people with jobs where security is paramount, for example, journalists, humanitarians, activists or special services working in unfriendly regimes, a phone that has been hacked via an app could put life at risk. For others, the risk of individual's private information or commercial data being accessed will damage an organisation's brand integrity and share price.

> This latest case of a serious vulnerability in a consumer-grade app highlights the dangers of using free apps, and that they are simply not robust enough for business"
> *David Holman, Director, Armour Comms*

David Holman, Director at Armour Comms said; "This latest case of a serious vulnerability in a consumer-grade app highlights the dangers of using free apps, and that they are simply not robust enough for business. While such apps claim that they are secure because they are encrypted, there is so much more to security than just encryption. Encryption is rarely the weakest link, and therefore, unlikely to be targeted by hackers.
"While this particular exploit may have been to target people with specific jobs, there are various other everyday hacks that can be executed relatively easily by low level criminals against these types of product that put users' data at risk. Breaches of GDPR are a risk to every type of business and come with significant fines." (i)

In 2018, German automotive supplier Continental AG banned its workers from using the messenger services WhatsApp and Snapchat on company phones, due to concerns about GDPR compliance and general security. (ii)
Holman continued; "These free apps proliferate by stealth through organisations, unless firms take positive action, like in the case of Continental AG last year. There are enterprise-grade apps available that provide the same convenient user experience of consumer grade apps, while keeping the user in control of their data and metadata. Some of these apps, like Armour Mobile, have been certified by the National Cyber Security Centre (NCSC), so users can be confident that the software is secure by design."

Armour Comms' solutions for secure communications work on everyday smartphones, tablets and Windows 10 desktops. With the same usability as consumer-grade apps, and with significantly enhanced security, Armour Mobile supports voice calls, video calls, one-to-one and group messaging, voice and video conference calls, file attachments, sent/received/read

message status and message ‘burn’ (automatic timed deletion).
Using a FIPS 140-2 validated crypto core, Armour Mobile has been awarded many certifications including CPA (Commercial Product Assurance) from the NCSC and is included in the NATO Information Assurance catalogue.

(i) https://www.armourcomms.com/2018/07/31/free-apps-you-might-get-more-than-you-bargained-for/?cat-slug=10
(ii) https://www.cnbc.com/2018/06/05/continental-bans-facebooks-whatsapp-and-snap-incs-snapchat.html

Andreina West
PR Artistry
+44 1491 845553
email us here
