EIN PRESSWIRE

A third of organisations use consumer-grade apps for business communications

Armour Comms Survey highlights alarming lack of awareness around mobile security

LONDON, UK, January 29, 2019 /EINPresswire.com/ -- Armour Communications, a leading provider of specialist, secure communications solutions, has published the results from its Mobile Communications Survey. The findings revealed that a third (32%) of organisations use consumer grade apps such as WhatsApp, SMS and Skype for business communications. Over two thirds (68%) use these apps regularly every day and over a third (36%) use the apps to discuss sensitive and confidential topics.

> The survey results highlight that many organisations are unaware of the pitfalls of using consumer grade-apps for handling sensitive corporate information”
>
> *David Holman, Director, Armour Comms*

The Survey also asked respondents to select from a list of different well known technologies, hacks and viruses which could be used to target mobile phones - nearly half (44%) answered incorrectly.
David Holman, Director at Armour Comms commented; “We see stories in the press on a regular basis about data leakage, sensitive customer data that is hacked by criminals, and yet, for most organisations managing how their staff are using their mobile phones remains a challenge. Consumer-grade apps, where the user has little control of what happens to their data, are often downloaded and used within organisations for sharing sensitive information, almost by stealth, because the IT/security department has no visibility of the apps being used.”

While viruses and malware on mobile phones are rare, tools for eavesdropping, such as IMSI catchers are increasingly within the reach of criminals that want to spy on others. Accordingly to the latest research by Ponemon, organisations have a nearly 28% chance of having a data breach in the next two years. In another report, social engineering is involved in over 90% of data breaches, where people are tricked into doing something, like clicking a link or providing data, to someone impersonating someone else.

Another pitfall for the unwary mobile user is WiFi which is often not as secure as people assume. All of these type of attacks are particularly easy to do with mobile phones where standard network encryption can be poor to non-existent, due to outdated infrastructure that is in parts well over 40 years old and probably no longer fit for purpose. This makes interception of mobile calls and messages much easier than it should be, and the user would be totally unaware until it was too late.

“In our experience end-users don’t deliberately put data at risk, they simply want to get on with their work, and extra security can cause an issue. The results from this survey highlight the fact that many organisations are unaware of the pitfalls of using consumer grade-apps for handling sensitive corporate information, whether that is intellectual property and trade secrets, customer information, or details of commercial transactions," added Holman.

Andreina West
PR Artistry
+44 1491 845553
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/475049871