

Latest Survey from Sotera Digital Reveals Shocking State of Mobile Phone Security in the Workplace

Sotera Digital Security, a leading US based provider of secure communications solutions, has released its Latest Survey Data.



NEW YORK, NY, USA, February 5, 2024

[/EINPresswire.com/](https://EINPresswire.com/) -- Sotera Digital

Security, a leading US based provider of secure communications solutions, has today released its findings from a survey it conducted among over 1,000 senior personnel of large businesses and multinational corporations across the globe.

“

The Sotera SecurePhone is the first and only out-of-the-box solution, purpose-built for ultimate professional privacy, which can and does claim one-hundred percent protection”

David Kay, CEO Sotera Digital

Sectors covered by the survey participants focused on those that require the need for ultra-secure and private communications - both regionally and worldwide - with clients, colleagues and suppliers; namely legal, pharmaceutical, media and corporate affairs, government, and blockchain / AI tech specialists.

The survey results provide key insights into current mobile phone security practices within the workplace, and reveal a startling lack of awareness among both professionals and their companies of the significant privacy threats with

standard smartphones and popular ‘secure’ messaging apps, despite a reportedly growing reliance on such for work-related communications.

[Key Findings https://soteradigital.com/survey-report/](https://soteradigital.com/survey-report/)

70% of the professionals surveyed were unaware that popular messaging apps are vulnerable to privacy attacks. Yet, 96% reported that their company allows the use of Signal and/or WhatsApp from their personal mobile phones for work communications, with over half (57%) reporting an increased usage of such apps compared to the previous year;

90% of the professionals surveyed place more importance on safeguarding the security and

privacy on their laptops than their mobile phones, despite 26% having had their mobile phone hacked in the past; 24% reported that their company doesn't have an official mobile phone policy, while a closer look at those that do reveals that approximately 1 in 4 such policies don't provide adequate guidance, such as the requirement of having a password to unlock the device;

87% of companies don't provide Mobile Device Management or Mobile Application Management to their employees - on both company and privately-owned devices that are used for work communications; Less than half of respondents update their device (48%) within 24 hours of a new software release, meaning over 50% are neglecting Android and IOS vulnerabilities which those updates attempt to patch.

Despite the prevalence of vulnerabilities, there is a significant lack of awareness among professionals regarding the susceptibility of popular smartphones and apps to privacy attacks. Findings signal an urgent call to organizations to reevaluate their mobile phone security protocols.

"Our survey demonstrates a clear gap in understanding and addressing phone security in the workplace. I am proud Sotera continues to raise critical awareness on standard smartphones and popular messaging apps like WhatsApp, often perceived as secure, that are in fact nowhere near one-hundred percent secure, with vulnerabilities that leave users and their organizations exposed to data breaches and privacy infringements", comments David Kay, CEO of Sotera Digital.

"The Sotera [SecurePhone](#) is the first and only out-of-the-box solution, purpose-built for ultimate professional privacy, which can and does claim one-hundred percent protection," David concludes.

The Sotera SecurePhone addresses the applications, operating system, and hardware - offering government-trusted, enterprise-dependable end-to-end mobile security and safeguarding sensitive data at every point. The multi-layered lockdown approach protects all three pillars of security, addressing vulnerabilities where standard smartphones cannot. For example, according to a recent report, over 75% of mobile security breaches occur through apps, and standard IOS and Android security features are 'added-on', leaving vulnerabilities at each integral layer.

The Sotera SecurePhone, trusted by government agencies and enterprises, delivers comprehensive end-to-end security for voice and text communications. Crafted specifically for professionals in mission critical industries, this state-of-the-art mobile device is fortified with the same operating system employed to safeguard the US Nuclear Arsenal - Integrity 178B.

Sotera's unparalleled level of security positions the SecurePhone as the premier choice for professions handling highly confidential data, uniquely able to promise peace of mind. In these sectors, any risk to phone security is non-negotiable.

The survey included 1,004 respondents (38% female, 56% male, 6% prefer not to say), between the ages of 20 and 55+ (24% 20-35, 46% 36-45, 21% 46-55, 9% 55+). Largest proportion of the sample were located in Europe (46%), but respondents were also located in the USA (27%), the UAE (17%) and SE Asia (12%). Respondents were CEO's (8%), COO's (14%), CTO/CDO's (32%), Partners (22%, law firms) and middle management (24%), spanning Blockchain / AI Tech entrepreneurs (38%), the legal sector (24%), Pharmaceutical / Meditech (11%), and Media / PR / Corporate affairs (11%).

About Sotera <https://soteradigital.com/>

Sotera Digital Security offers clients across the globe with end-to-end security for both voice communications and text messages. Led by a team of recognized mobility experts, Sotera is focused on delivering innovative, data privacy solutions that offer clients a competitive edge. The company's current offering, the Sotera Secure Communications service represents the successful engineering of multi-layered defense and security combining Integrity 178, the only operating system in the world to achieve NSA's highest certification level (EAL6+); propriety partitioned communication apps; and data transmission encryption.

For more information, for press interviews, and to receive the entire survey, please contact pr@soteradigital.com.

Bryan Feinberg
Amplifi / Plato
+1 551-574-2169

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/686334098>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.