

Growing privacy and security concerns in evolving Smartphones

Published on August 27, 2024

Document Date: Sun, Jan 11 2026 12:00:28 am

Category: ,English,International - ,Snippets

Show on website : [Click Here](#)

RKI Website !

As smartphones increasingly store our most confidential data, the need for robust security measures has never been greater, warns Vladislav Tushkanov, Research Director for Machine Learning Technology at cybersecurity firm Kaspersky. He emphasizes the importance of using security apps to guard against potential malware threats.

Tushkanov highlights the risks posed by AI assistants, which exist in two forms: on-device and online. While on-device assistants are generally safer as they don't require internet access, online assistants pose significant privacy risks. He advises against sharing confidential information with these online tools, as they may offer unreliable advice and expose personal data.

To protect sensitive information, Tushkanov recommends using strong passwords and enabling two-factor authentication. However, even these measures may not fully safeguard against data leaks, especially when chatbots and virtual assistants are involved. On-device assistants, while more secure, may still underperform due to the limited hardware capabilities of smartphones, potentially leading to misinformation.

He also cautions against making conversations too personal when interacting with AI chatbots, particularly those offering emotional support. These interactions could be used by app providers to enhance their models, increasing the risk of data misuse.

Tushkanov concludes by advising users to be cautious when installing apps, paying close attention to the permissions requested. He underscores the importance of relying on trusted apps and utilizing security solutions to defend against malicious software. Kaspersky, he notes, actively detects threats masquerading as clients of popular AI services, further underscoring the need for vigilant digital practices.