# The evolving landscape of IoT security and Google Assistant's uncertain future



The Internet of Things (IoT) has increasingly become an integral aspect of modern living, with devices such as smartphones, smart thermostats, security cameras, and various connected gadgets enhancing comfort, convenience, and overall efficiency within homes. However, as the prevalence of these devices surges, they also bring an array of security risks that users must navigate.

The growing concern around IoT security is underscored by a notable incident from 2016 when the Mirai botnet exploited millions of unsecured devices, including cameras and DVRs, to execute significant DDoS attacks, disrupting major web platforms like X, Spotify, and Netflix. More recently, in 2022, researchers uncovered a vulnerability in Amazon’s Alexa devices, labelled Alexa versus Alexa (AvA). This flaw potentially allowed attackers to issue unauthorized commands to smart speakers, opening the door for home automation control, making unapproved purchases, and engaging in eavesdropping activity.

Despite their daily use, many consumers remain unaware of the security implications associated with smart home devices. Common vulnerabilities include weak or default passwords, infrequent software updates, unsecured Wi-Fi connections, inadequate privacy protections, and weaknesses in third-party integrations. These gaps can enable hackers to exploit devices, compromising users' privacy and data security.

To enhance the security of IoT devices, experts recommend several best practices. Key measures include changing default passwords to more robust and unique alternatives, enabling two-factor authentication (2FA) where possible, and regularly updating software and firmware to address known vulnerabilities. Users are also advised to secure their Wi-Fi networks, disable unused features on their devices, segment their networks, and limit third-party integrations to trustworthy services.

Despite the potential security risks, broader regulatory frameworks are being established to address privacy concerns associated with IoT devices. For instance, the IoT Cybersecurity Improvement Act in the USA mandates that federal IoT devices comply with stringent cybersecurity criteria. Meanwhile, the UK has introduced a Code of Practice for Consumer IoT Security, advocating for secure passwords and regular software updates. Additionally, legislation in regions like the European Union and California aims to bolster user rights over their personal data and enforce stringent data protection measures.

As IoT technology progresses, the anticipation of newer advancements looms large, urging both regulators and manufacturers to enhance security measures further and protect user privacy.

In another realm of smart technology, Google’s recent strategic shift towards its advanced AI model, Gemini, has sparked considerable speculation among users of Google Assistant-enabled devices. The potential for phasing out the Google Assistant raises concerns for millions of users, who rely on these smart speakers for everyday tasks such as managing schedules or controlling home environments.

Google's aggressive integration of Gemini, touted for its superior conversational abilities and understanding of complex tasks, has left users uncertain about the fate of their existing Google Assistant-powered devices. Concerns are mounting among users, such as Sarah, a busy working mother, who states, "I invested in a smart home ecosystem built around Google Assistant. The thought that these devices might stop working or lose their key features is really frustrating."

The uncertainty surrounding whether existing devices will receive updates to support Gemini, or if they will face functional obsolescence, breeds apprehension. This could result not only in financial loss for consumers but also contribute to the growing issue of electronic waste.

While Google has not definitively announced a timeline for phasing out Google Assistant, its clear focus on the Gemini model implies that such a transition is on the horizon. Users are left in limbo, questioning whether to continue investing in devices associated with the current ecosystem or seek alternatives. This situation complicates the future of many third-party manufacturers that base their products on Google Assistant technology.

To mitigate potential disruptions, users might consider diversifying their smart home integrations to include devices that support multiple ecosystems or voice assistants, preserving some functionality during the transition period. However, the onus is on Google to communicate a clear roadmap regarding the transition from Assistant to Gemini, outlining device compatibility and support timelines, thus reassuring users about their investments.

As advancements in AI technology continue to unfold, the landscape of smart devices promises to evolve. However, inclusive strategies that deliver clarity and maintain support for current users will be essential in preserving trust and customer loyalty during this inherently transformative time.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.kaspersky.com/about/press-releases/kaspersky-unveils-an-overview-of-iot-related-threats-in-2023> - This URL supports the claim about IoT-related threats, including DDoS attacks and vulnerabilities in IoT devices. Kaspersky's research highlights the increasing risks associated with IoT security.
* <https://www.jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025> - This article provides data on IoT security risks, including common vulnerabilities such as weak passwords and outdated software, which aligns with the discussion on IoT security imperatives.
* <https://www.zscaler.com/resources/2023-threatlabz-enterprise-iot-ot-threat-report> - The Zscaler ThreatLabz report details the increasing threats to IoT devices, including a massive rise in malware attacks, reinforcing the security concerns discussed in the article.
* <https://www.gov.uk/government/news/new-laws-to-protect-millions-of-users-of-smart-devices-from-cyber-attacks> - This URL supports the introduction of regulatory frameworks like the UK's Code of Practice for Consumer IoT Security, which advocates for enhanced device security measures.
* <https://www.congress.gov/bill/116th-congress/house-bill/1668> - This legislation document outlines the IoT Cybersecurity Improvement Act in the USA, which mandates federal IoT devices comply with stringent cybersecurity criteria.
* <https://ai.googleblog.com/2022/05/introducing-gemini-next-generation.html> - This blog post introduces Google's Gemini AI model, highlighting its superior conversational capabilities and its potential impact on Google Assistant-related devices.