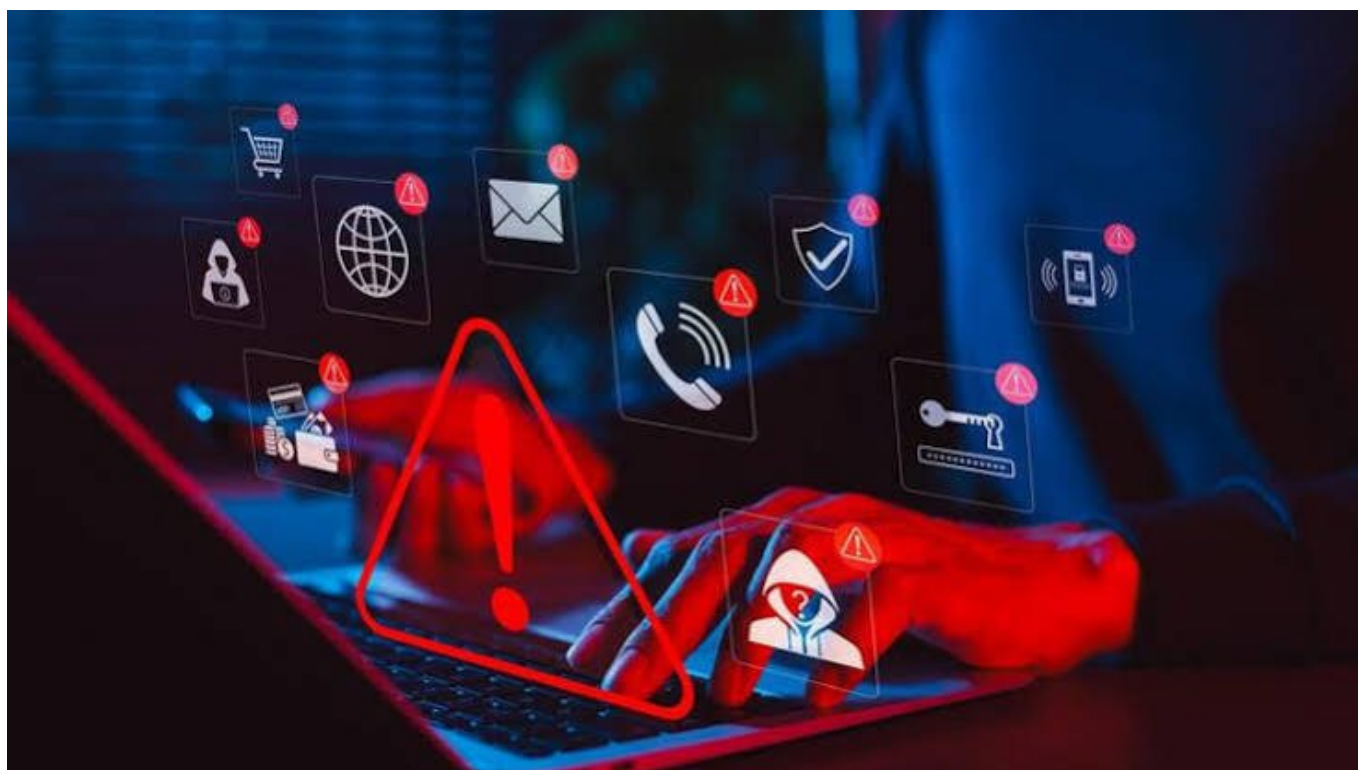


NEWS | ARTIFICIAL INTELLIGENCE

Dashlane Launches AI-Powered Scam Protection to Block Phishing Threats in Real Time

The new feature analyzes webpages on-device to detect suspicious activity and protect users from entering credentials, payment details, and other sensitive information on phishing sites.

By **Ankit Kankar** | September 13, 2026



Picture Courtesy | Public Domain

Dashlane, the credential security leader, announced the launch of AI-powered **Scam Protection**, a new feature for Dashlane personal plan users that actively protects them from entering their credentials, credit card information, or other sensitive data on phishing websites, even when they have no saved logins to compare against.

Unlike traditional anti-phishing solutions that only intervene when users attempt to autofill or paste a saved credential, Scam Protection uses a patent-pending, proprietary AI model that analyzes every page in real time, intervening at the exact moment the user is at risk, blocking threats before users interact with them.

"AI has made it easier for scammers to quickly create convincing phishing campaigns that now reach consumers through social media platforms, texts, email and more," said Christophe Frenet, Chief Product Officer at Dashlane. "Scam Protection brings users peace of mind as a specially-trained digital detective that spots what humans can't, stepping in and alerting busy people who, naturally, are not vigilantly checking every site they visit."

Why it matters

- **Protection that doesn't depend on the vault:** Phishing attacks increasingly target first-time interactions: fake checkout pages, fraudulent job applications, counterfeit account sign-ups, where users have no saved credentials. Vault-based phishing alerts that only trigger on URL mismatches leave these scenarios completely unprotected.
- **Nor static domain lists:** AI has enabled attackers to rapidly spin-up new, increasingly realistic phishing campaigns with AI, making solutions reliant on known phishing domain lists inadequate to deal with the velocity and breadth of scams users face. In fact, 74 percent of IT leaders report that AI poses an increased threat to password security, according to the 2025 Dashlane State of Credential Security Report.

Intelligent, adaptive phishing protection

Dashlane has long offered vault-based phishing alerts that prevent autofill on mismatched domains, a feature now standard across password managers. Scam Protection stands apart because of its AI model, which analyzes 79 webpage attributes in real-time, including URL anomaly patterns, excessive external links, hidden images, and more, to determine whether a web page is suspicious

as the user browses. This proactive approach protects users in scenarios where credential-matching cannot: entering a credit card on a fake shopping site, creating an account on a fraudulent service, or submitting personal information to a scam job posting.

In accordance with Dashlane's zero-knowledge approach, Dashlane's analysis of the web page occurs entirely on the user's device, without transmitting browser data externally. No user data is leveraged to train the AI model, ensuring complete privacy protection.

Read online: <https://worldbusinesswatch.com/news/31/147/dashlane-launches-ai-powered-scam-protection-to-block-phishing-threats-in-real-time.html>

© 2026 World Business Watch. All rights reserved.