DASHLANE

AI Phishing Alerts

Build a phishing-resistant enterprise with real-time protection against the most advanced phishing threats

The challenge: Outsmarting AI-powered phishing

Phishing remains the #1 cause of breaches[1] and AI is making attacks harder to spot.

Sophisticated lures bypass security training, email filtering, and blocklists, leaving employees exposed the moment they land on a malicious site.

Traditional vault-based password managers don't:

- Assess if sites are malicious through an proprietary AI model and alert employees
- Give IT and security teams actionable phishing insights or customizable controls
- Protect employees who aren't logged in or haven't deployed the extension

The result? Dangerous blind spots across the organization.

IT and security leaders need a last line of defense that outsmarts AI-powered phishing and works where the credential compromise actually occurs: The browser.

The solution: AI phishing alerts

Built into the Dashlane Omnix™ intelligent credential security platform, AI phishing alerts notify employees about phishing risks the moment they visit a suspicious website in the browser.

With phishing threats continuing to bypass traditional phishing protections, this closes a critical gap in the phishing attack lifecycle.

They also give admins proactive threat insights and control to eliminate blind spots and strengthen organizational resilience.

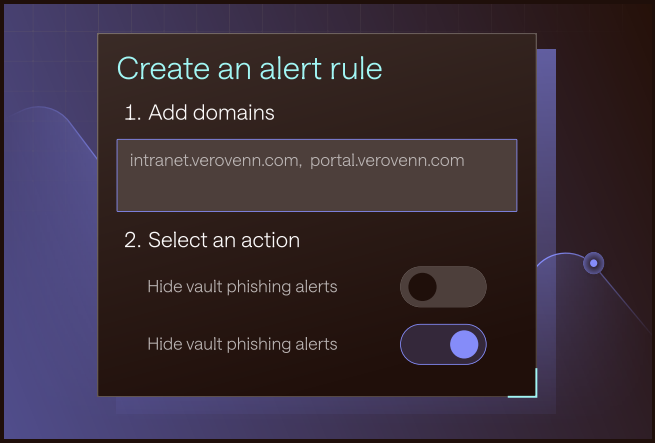
54% The average click-through rate for AI-crafted phishing emails[2]

1: IBM, "What is phishing?"
2: Heiding et al., "Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns," 2024

DASHLANE

Why AI phishing alerts are different

- Real-time detection of phishing sites before employees can enter their credentials
- Automated alerts that protect employees and reduce successful phishing attempts—no IT effort required
- Admin visibility into risky domains and user behavior with actionable insights
- Customizable controls that enable admins to implement up to 200 rules to suppress alerts on trusted domains



How it works:

1. An employee lands on a website with a login form
2. Dashlane's proprietary AI model analyzes 75+ domain attributes—from page structure to hidden elements—in less than half a second
3. If suspicious, the employee receives an in-browser alert before they enter their credentials
4. Admins also receive in-depth reporting and can view phishing exposure trends in their Omnix dashboard

Start protecting every login

AI phishing alerts are part of Omnix, the only platform that goes beyond the boundaries of a traditional password manager with active, browser-based phishing defense for every single login, even for employees who don't use Dashlane.

The platform protects against the entire lifecycle of a credential-based threat, providing end-to-end coverage—before credentials are exposed.

Get advanced phishing protection for every login

Request an Omnix demo