Keeper Security Introduces Verify Mode and New Browser Controls to Prevent Phishing and Credential Misuse

New feature validates credential use at the point of entry, helping enterprises stop phishing attacks before credentials are exposed

LONDON, UNITED KINGDOM, April 27, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge identity security and Privileged Access Management (PAM) platform, today announces the release of Verify Mode, a new anti-phishing capability in version 17.8 of its browser extension. Verify Mode provides real-time validation of where credentials are being entered, helping prevent users from entering passwords into malicious or unrecognised websites.

As phishing attacks continue to grow in sophistication and frequency, credential theft remains one of the most effective paths for unauthorised access into enterprise systems. According to research from Verizon, 60% of breaches involved a human element, such as credential abuse or phishing scams. Modern organisations operating across cloud, hybrid and remote environments face increasing exposure to these threats. The new, optional Verify Mode introduces an active control at the point of credential entry, reducing reliance on user judgment alone.

“Phishing attacks succeed by targeting the moment that users enter their credentials,” said Darren Guccione, CEO and Co-founder of Keeper Security. “Even well-trained employees can be deceived by convincing, malicious websites. Verify Mode changes that by validating credential use in real time, ensuring passwords are only entered on trusted domains. It shifts credential security from passive storage to active protection.”

Real-Time Protection Against Credential Misuse

Verify Mode monitors password paste activity in the browser and verifies that the destination site matches the corresponding record stored in the user’s Keeper Vault. If a mismatch is detected, users receive an immediate warning before credentials are submitted, with clear details and the option to proceed or cancel.

Verify Mode includes configurable protection levels to align with organisational risk tolerance:
 Medium: Alerts users when credentials copied from the vault are pasted into a different site than the one saved

 High: Warns users when a password is pasted into any site not stored in the vault
 Maximum: Requires confirmation before pasting passwords on any site, including trusted ones

These controls allow security teams to balance strong protection with a seamless user experience across roles and environments.

Extending Zero Trust To Credential Usage

Verify Mode extends Keeper's zero-trust approach beyond credential storage to real-time enforcement of credential usage. By validating every interaction, organisations gain stronger control over how and where credentials are used.

Key enterprise benefits include:
 Reduced risk of credential-based attacks: Stops phishing at the point of entry
 Stronger security posture: Enforces continuous validation aligned with zero-trust principles
 Enhanced compliance readiness: Demonstrates enforcement of secure credential practices
 Reduced human error: Mitigates one of the leading causes of breaches

Verify Mode further bolsters Keeper's unified identity security platform, which combines password management, secrets management, endpoint privilege management, AI-powered threat detection and privileged access controls into a single, cloud-based solution designed for modern enterprise environments.

As identity-based attacks continue to target users across SaaS applications, cloud and remote environments, organisations need real-time controls. Verify Mode delivers this protection directly at the point of credential use without disrupting the user experience.

Other features in Browser Extension release 17.8 include prompting users to disable the built-in browser password manager and support for custom fields. Upon first login or installation of the KeeperFill Browser Extension, a prompt will appear asking users to set Keeper as their default password manager. This optional step prevents interference from the browser's native password manager, guaranteeing the best possible autofill experience without requiring manual adjustments.
Users can now also add custom fields directly to records from the browser extension, no longer requiring a switch to the web vault for editing. An unlimited number of custom fields can be added and easily reordered using drag-and-drop, similar to the existing feature on web and mobile vaults. These fields can store sensitive information, like security questions, PINs or private notes regarding logins, and are masked by default for privacy.

Verify Mode is now available in the Keeper browser extension for enterprise users. Administrators can enable and configure protection levels through the Keeper Admin Console. To learn more, visit KeeperSecurity.com.

###

About Keeper Security
Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organisations to defend against modern adversaries at KeeperSecurity.com.

Learn more: KeeperSecurity.com (https://www.keepersecurity.com/?&utm_medium=press_release&utm_campaign=Communications)

Charley Nash
Account Manager
charley@eskenzipr.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok
X
