

Keeper Security Calls for Action: Week Three of Cybersecurity Action Month Spotlights the Importance of Enabling MFA

Keeper encourages individuals and organisations to recognize Cybersecurity Action Month by enabling Multi-Factor Authentication (MFA) everywhere possible

LONDON, UNITED KINGDOM, October 14, 2024

/EINPresswire.com/ -- Week three of Cybersecurity

Awareness Action Month is upon us, and [Keeper](#)

[Security](#) is urging consumers and businesses alike to

adopt and enforce fundamental cybersecurity

practices. The leading provider of zero-trust and zero-

knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and

remote connections, announces that this week's actionable step to proactively strengthen online

security is to enable Multi-Factor Authentication (MFA). Building on the prior weeks' tips –

spotting phishing scams and using strong passwords with a password manager – MFA adds

another critical layer of protection to help secure your accounts and data.

Strong authentication practices, such as using unique passwords and implementing MFA, are essential for enhancing online security and mitigating cyber risks. MFA adds a critical extra layer of protection, making it harder for malicious actors to compromise accounts. Even if an account's login credentials are compromised, the cybercriminal would not be able to breach the account without the additional authentication step. Yet, despite its proven benefits, MFA is still widely underutilised both by individuals and organisations, with many high-profile examples of damaging breaches due to the absence of MFA.

“At Keeper Security, we launched Cybersecurity Action Month to usher in the necessary shift from awareness to real action in adopting cybersecurity best practices both at work and at home,” said Darren Guccione, CEO and Co-founder, Keeper Security. “Implementing MFA across all accounts significantly strengthens access controls and credential management for enterprises while protecting consumers from malicious hackers targeting their devices, accounts and sensitive data. Enforcing fundamental best practices like enabling MFA is key to securing our digital world.”

As the cyber threat landscape evolves, including the rise of AI-powered attacks, MFA can help



thwart these sophisticated attacks. MFA ensures that even advanced techniques – such as deepfakes or compromised credentials – face additional hurdles for access. Thirty-six percent of respondents to Keeper Security's [2024 Insight Report](#) shared that deepfake technology is among the top emerging attack vectors they're witnessing first hand at their organisations, highlighting the importance of addressing this threat.

As IT leaders and consumers take action to enforce MFA this Cybersecurity Awareness Action Month, it's important to keep in mind that not all MFA methods are equally effective. Traditional methods, such as SMS, are less secure compared to more robust options like authenticator apps or hardware keys. The use of a password manager can mitigate this security risk by storing and autofilling MFA codes with a built-in authenticator app – providing a seamless user experience and protecting against attacks like social engineering or SIM swapping.

Keeper kicked off Cybersecurity Action Month by spotlighting the criticality of strong passwords and using a reliable password manager to protect them. A solution like Keeper addresses these crucial needs and simplifies the MFA process for end users. With its secure storage and generation of MFA codes, a password manager can help both organisations and individuals efficiently implement and enforce the use of MFA.

As Cybersecurity Action Month continues, follow Keeper Security for more action items and resources to fortify your digital life. Check out our [image collection](#) to see how the Keeper team is taking action this month.

###

About Keeper Security

Keeper Security is transforming cybersecurity for people and organisations around the world. Keeper's affordable and easy-to-use solutions are built on a foundation of end-to-end encryption, zero-trust and zero-knowledge security to protect every user on every device. Our next-generation privileged access management solution deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging.

Learn more: KeeperSecurity.com

Charley Nash
Eskenzi PR
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/751022027>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.