EINPRESSWIRE

Keeper Security Shares Essential Cybersecurity Practices for Preparedness Month

A significant portion of data breaches could be prevented with stronger password management and multi-factor authentication

LONDON, UNITED KINGDOM, August 29, 2024 /EINPresswire.com/ -- For Preparedness Month in September, Keeper Security, a leading provider of zero-trust and zero-knowledge cybersecurity software, urges businesses to prepare for the rising tide of cyber threats by prioritising fundamental cybersecurity practices. With more sensitive data being stored online, the risk of breaches and exploitation is at an all-time high. In a recent survey conducted by Keeper Security, 92% of U.S. IT and security professionals reported a year-over-year increase in cyber attacks targeting their organisations. To defend against the most common cyber threats, as well as emerging threat vectors, fundamental, yet often neglected, cybersecurity best practices must be prioritised.

> “
> During National Preparedness Month, it’s vital for organisations to prioritise fundamental security best practices.”
>
> *Darren Guccione, CEO and Co-Founder of Keeper Security*

Strengthening data security processes is a crucial step to mitigate organisational risk in today’s evolving threat landscape. Key practices such as implementing robust data encryption, regularly updating and patching systems, and implementing strong access controls can help protect sensitive information from unauthorised access.

Keeper advises organisations of all sizes to implement the following fundamental protections:

- Establish regular employee training on cybersecurity best practices and phishing awareness.
- Implement strong access controls and conduct regular security audits to mitigate the risk of insider threats.
- Strengthen account protection by adopting a password management solution and enforcing the use of MFA.

Conduct Regular Cybersecurity Training for Employees

Just as preparedness is key to mitigating the risk and potential damage associated with natural disasters, it's also essential in cybersecurity. Regular employee training and education on cybersecurity best practices are crucial for protecting an organisation from evolving cyber threats. Verizon's 2024 Data Breach Investigations Report reveals 68% of breaches involved a non-malicious human element, such as a person falling victim to a social engineering attack or making an error. This can lead to devastating consequences.

A significant majority of respondents to Keeper's recent survey – 61% – identified phishing as one of the most common cyber threats facing their organisations, with more than half (51%) reporting a significant increase in the frequency of these attacks. The human element is often the most vulnerable link in the attack chain, underscoring the criticality of educating users and conducting phishing simulations to enhance overall security awareness.

By training employees to recognize and respond to simulated phishing attacks, organisations can effectively prepare their frontline defenders to question unexpected notifications, report suspicious activity promptly and foster a culture of vigilance – ultimately strengthening their cybersecurity posture.

Beware of Insider Threats, Both Malicious and Unintentional

Preparedness extends to understanding and mitigating insider threats, whether malicious or unintentional, which pose significant risks to organisations. Keeper's survey found that 40% of respondents experienced a cyber attack originating from an employee. To mitigate these risks, organisations should implement strong access controls and offboarding processes, provide comprehensive employee training and conduct regular security audits. Deploying a Privileged Access Management (PAM) solution can further enhance security by centralising and controlling access to sensitive systems and data, reducing the risk of unauthorised access and data breaches.

Implement Processes and Technologies To Prevent and Thwart Attacks

In a world where data breaches have become increasingly common, preparedness is essential. Creating strong, unique passwords for each account remains a critical first line of defence against unauthorised access, yet many organisations and individuals fail to follow password best practices. Keeper's survey found that nearly 40% of respondents identified password reuse as their most common password-related error. A password manager creates and stores high-strength, random passwords for every website, application and system, helping prevent the domino effect in which the compromise of one account leads to further unauthorised access.

In addition, password managers can help avoid incidents of stolen passwords, which impact 52% of IT and security leaders. These tools also support strong forms of Multi-Factor Authentication

(MFA), such as an authenticator app, to add additional layers of protection to accounts, making unauthorised access significantly more difficult. When selecting a password manager, it’s important to prioritise providers that offer transparent security architecture, zero-knowledge and zero-trust infrastructure, and certifications like SOC 2, ISO 27001, 27017 and 27018, as well as FedRAMP Authorization, to ensure the highest level of protection.

“During National Preparedness Month, it’s vital for organisations to prioritise fundamental security best practices," said Darren Guccione, CEO and Co-Founder of Keeper Security. "By being prepared with strong password management, enabling multi-factor authentication and staying vigilant against phishing scams, we can significantly reduce our vulnerability to cyber threats and protect our sensitive information.”

As National Preparedness Month highlights the importance of being ready for all types of emergencies, now is the time for organisations to assess their cybersecurity preparedness. By taking proactive measures and following fundamental cybersecurity practices, they can significantly reduce their vulnerability to cyber threats and protect valuable information.

###

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.

Charley Nash
charley@eskenzipr.com
Eskenzi PR