EINPRESSWIRE

Keeper Security Urges Businesses to Strengthen Cybersecurity During Home Office Safety and Security Week

In honour of Home Office Safety and Security Week, Keeper® offers critical insights into the evolving risks businesses face in remote work environments

LONDON, UNITED KINGDOM, January 14, 2025 /EINPresswire.com/ -- As businesses continue to embrace remote work and evolve hybrid work structures, cybercriminals are increasingly targeting the vulnerabilities created by these decentralised environments. During Home Office Safety and Security Week, Keeper Security – the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections – is emphasising the need for stronger cybersecurity practices to protect distributed workforces and sensitive business data.

> “
> Remote and hybrid work environments are here to stay, and with these distributed workforces comes an essential need for a comprehensive approach to cybersecurity.”
>
> *Darren Guccione, CEO and Co-founder of Keeper Security*

“Remote and hybrid work environments are here to stay, and with these distributed workforces comes an essential need for a comprehensive approach to cybersecurity,” said Darren Guccione, CEO and Co-founder of Keeper Security. “Organisations must be proactive in securing their on-premise and remote digital environments and privileged accounts, to prevent breaches, protect sensitive data and maintain trust with customers.”

Cybersecurity Risks in Remote Work Environments

Remote and hybrid work has exponentially expanded the attack surface for businesses, with employees relying on personal devices, home networks and cloud-based services that may lack adequate security measures. Cybercriminals are taking advantage of this decentralisation, targeting unsecured networks and unprotected endpoints. The global cost of a data breach now averages $4.88 million, highlighting the significant financial risks posed by these security gaps.

Alongside the growing number of attack vectors, insider threats – whether intentional or accidental – pose significant risks to organisational security. Phishing scams, which have risen sharply in recent years, are one of the primary methods attackers use to gain access to systems and data. Weak passwords, a lack of Multi-Factor Authentication (MFA) and insufficient monitoring make it easier for attackers to exploit these vulnerabilities, with breaches often going undetected for months.

Without a comprehensive PAM solution, the breach of any employee – remote or in the office – can put an organisation's most sensitive data and infrastructure at risk. As businesses reflect on their cybersecurity posture during Home Office Safety and Security Week, the need for stronger security measures has never been clearer. Adopting technologies like password and passkey manager, PAM and implementing a zero-trust security model is critical to managing access to sensitive data and minimising the risk of unauthorised entry.

Addressing Remote Work Security Challenges

To effectively protect remote work environments, businesses must implement a layered approach to cybersecurity which includes:
- Restricting access to critical systems: Ensuring that only authorised personnel can access sensitive data based on their specific roles.
- Adopting zero-trust security models: Verifying every access request, regardless of where it originates, to prevent unauthorised access.
- Enhancing credential security: Using secure password management tools to ensure passwords are properly stored, rotated and not reused across systems.
- Ongoing employee education: Regularly training employees to recognise phishing attempts and practice good security hygiene.
- Real-time monitoring: Investing in tools to monitor network activity and immediately address any suspicious behaviour.

By leveraging these practices and investing in effective cybersecurity solutions, organisations can reduce their exposure to the most common and damaging threats in remote work environments.

KeeperPAM: Enhancing Security for Remote Workforces

As organisations face mounting cybersecurity challenges, adopting integrated solutions like KeeperPAM® can significantly enhance security across remote teams. KeeperPAM is designed to mitigate the risks associated with remote and hybrid work by providing robust privileged access management features, such as Role-Based Access Control (RBAC) and Just-In-Time (JIT) access. These capabilities ensure that sensitive systems and data are accessible only to authorised users, minimising the risk of unauthorised access.

KeeperPAM's real-time monitoring also enables businesses to track user sessions, identify

suspicious activity and maintain an audit trail for compliance. This comprehensive solution, which meets the highest security standards including SOC 2 Type II compliance, FedRAMP Authorisation and ISO 27001, 27017 and 27018 certifications, helps businesses manage privileged access securely while integrating seamlessly into existing infrastructures.
As Home Office Safety and Security Week highlights, it’s vital for organisations to stay ahead of cybercriminals by embracing advanced security practices and tools that mitigate risks in distributed work environments.

For more information on how to protect your organisation and distributed workforce, visit www.keepersecurity.com.

###

About Keeper Security
Keeper Security is transforming cybersecurity for people and organizations globally. Keeper’s intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Our zero-trust privileged access management platform 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 organizations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging. Learn how our zero-trust and zero-knowledge solutions defend against cyber threats at KeeperSecurity.com.

Learn more: KeeperSecurity.com
Follow Keeper: Facebook Instagram LinkedIn X YouTube TikTok

Charley Nash
Eskenzi PR
email us here